Active Directory

Document technique sur l'Active Directory

Par

Grégoire LE BARON

Table des matières :

1- Introduction

Une entreprise peut compter plusieurs milliers de salariés. Par conséquent il est important de pouvoir centraliser toute la gestion des profils, des droits etc… en un seul endroit. Ce document technique vise à expliquer comment nous pouvons créer un domaine contenant des utilisateurs ayant chacun des droits spécifiques.

Pour cela, nous nous baserons sur une organisation prédéfinie.

2- Prérequis

Nous allons avoir besoin de minimum deux machines virtuelles (MV), une qui permettra de faire tourner Windows Server 2019 (WS19) qui hébergera l'Active Directory (AD), et une autre qui permettra de faire tourner Windows 10 Enterprise (W10E), représentant un salarié.

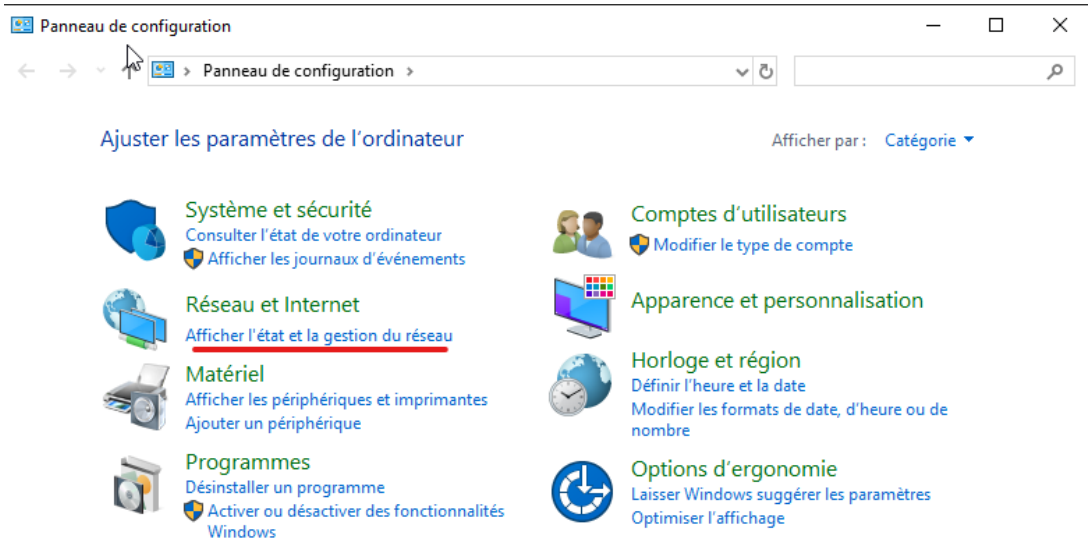
La mise en place de ces machines virtuelles suit la documentation technique concernant la création de machine virtuelle. La seule différence est l'utilisation d'une image .iso différente (Une pour WS19 et une pour W10).

3- Ipssi.lan

a) Créer le domaine

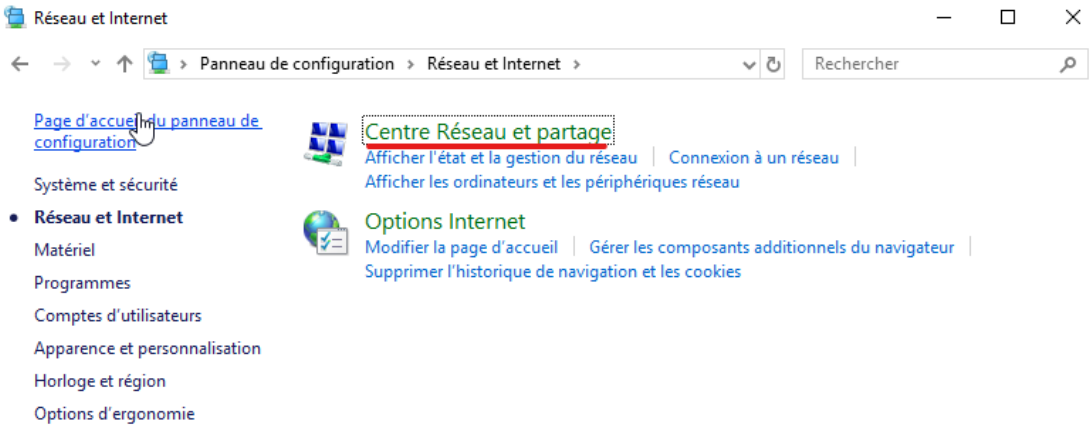
Nous allons maintenant créer un domaine appelé Ipssi.lan.

Etape 1



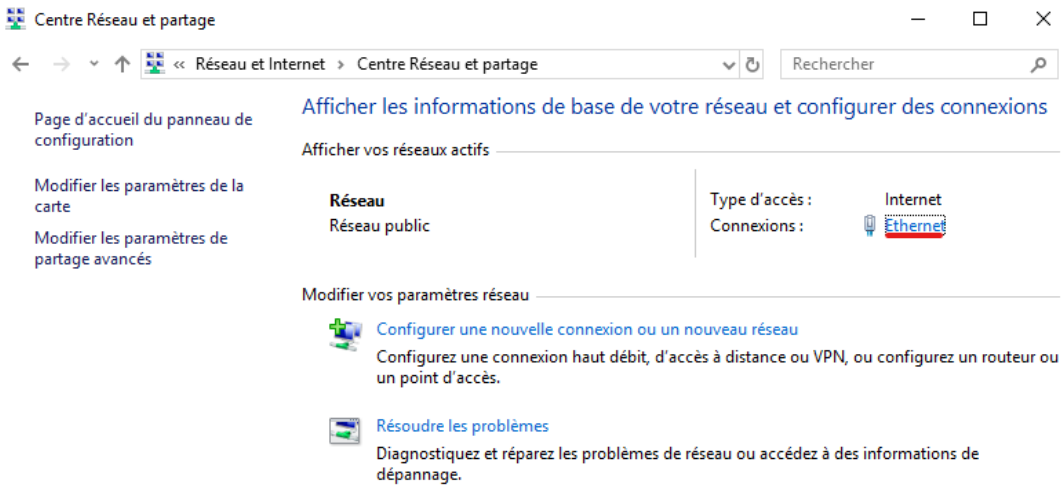
Sur WS19, nous nous rendons dans le « panneau de configuration » puis « Afficher l'état et la gestion du réseau ».

Etape 2



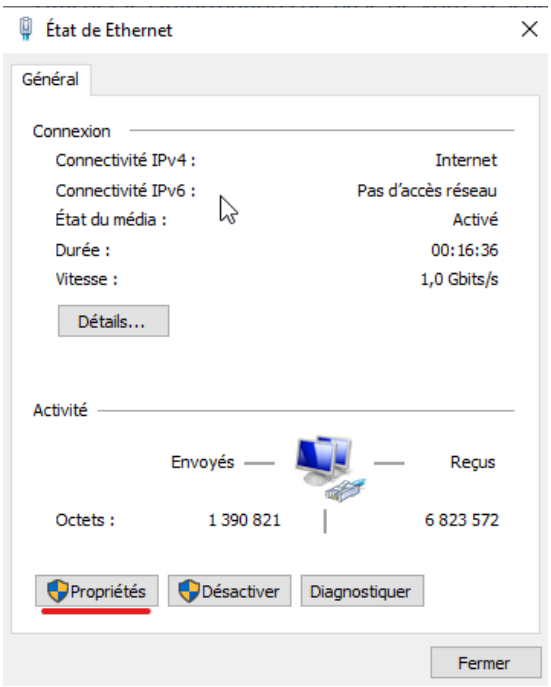
Ensuite nous cliquons sur « Centre de Réseau et partage ».

Etape 3



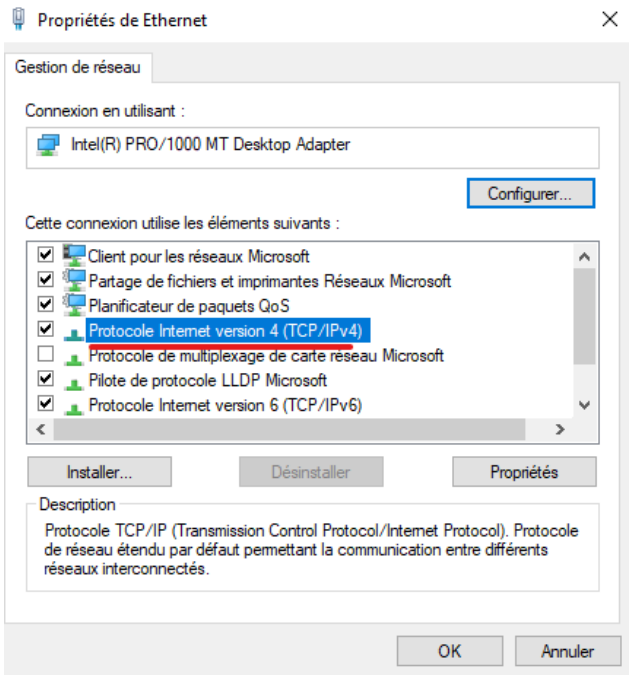
Nous cliquons sur « Ethernet ».

Etape 4



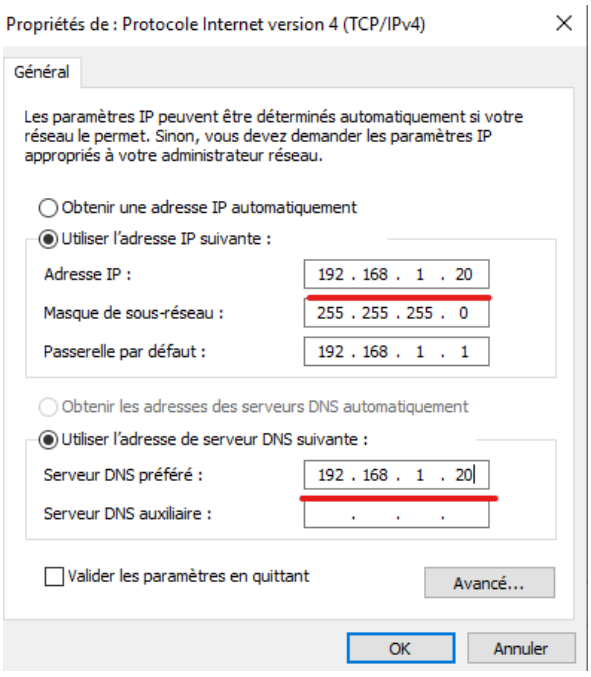
Nous cliquons sur « Propriétés ».

Etape 5



Nous double-cliquons sur « Protocole Internet version 4 (TCP/IPv4).

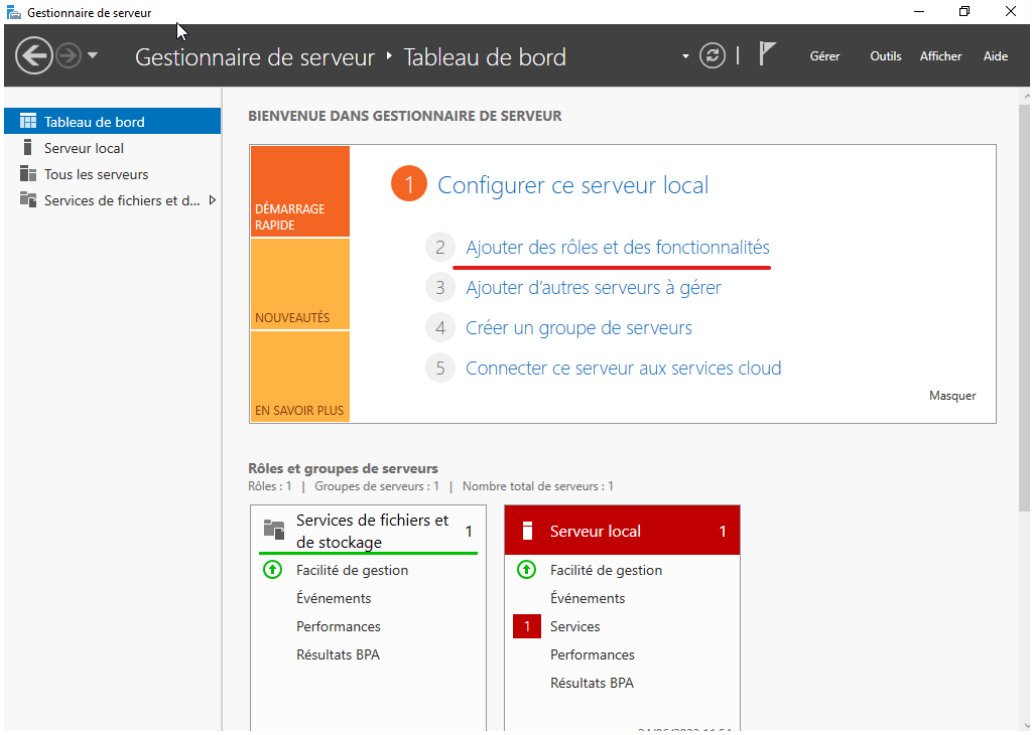
Etape 6



Nous rentrons les informations comme sur l'image ci-dessus. Concernant W10E, l'adresse IP sera 192.168.1.20. Les autres informations sont similaires.

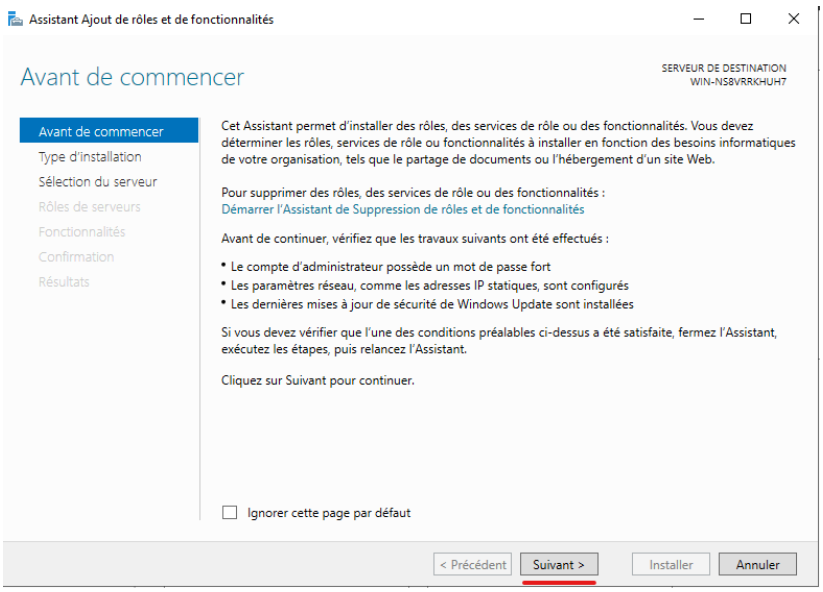
Il est important que l'adresse IP du Serveur DNS préféré corresponde à l'adresse IP de WS19 car il héberge l'AD.

Etape 7



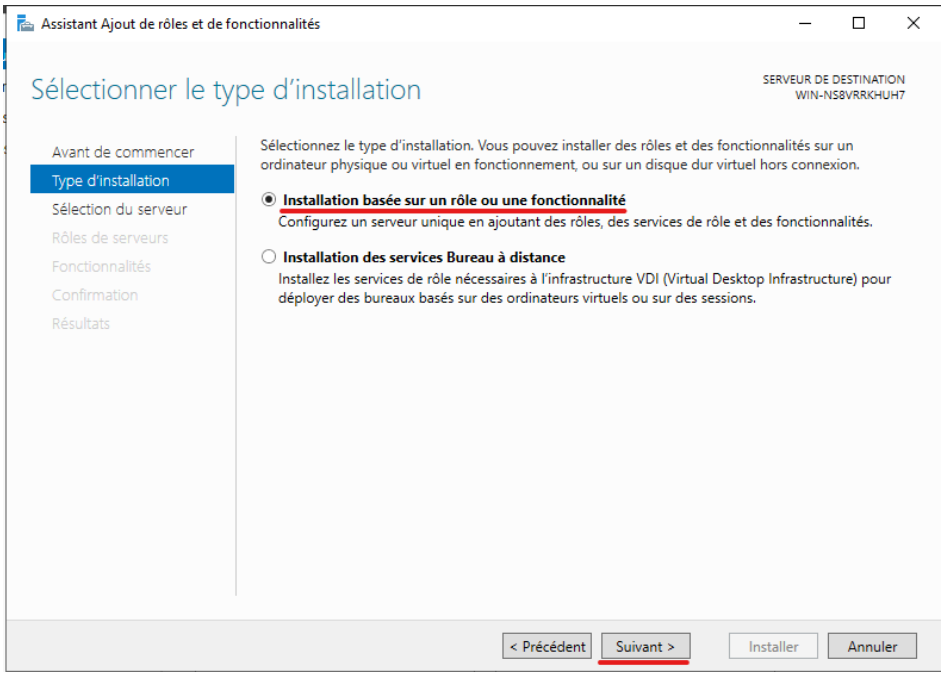
Nous nous rendons maintenant dans le gestionnaire de serveur puis nous cliquons sur « Ajouter des rôles et des fonctionnalités.

Etape 8



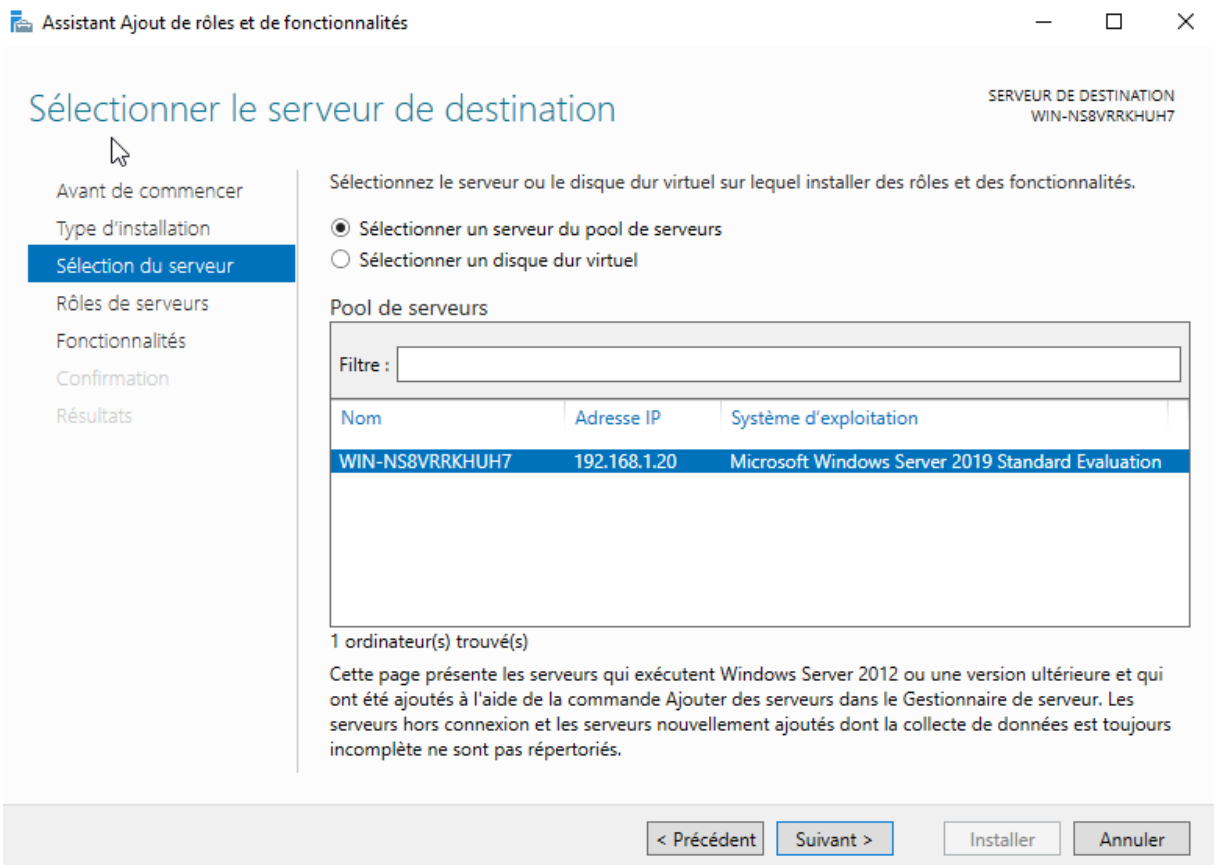
Nous cliquons sur « suivant ».

Etape 9



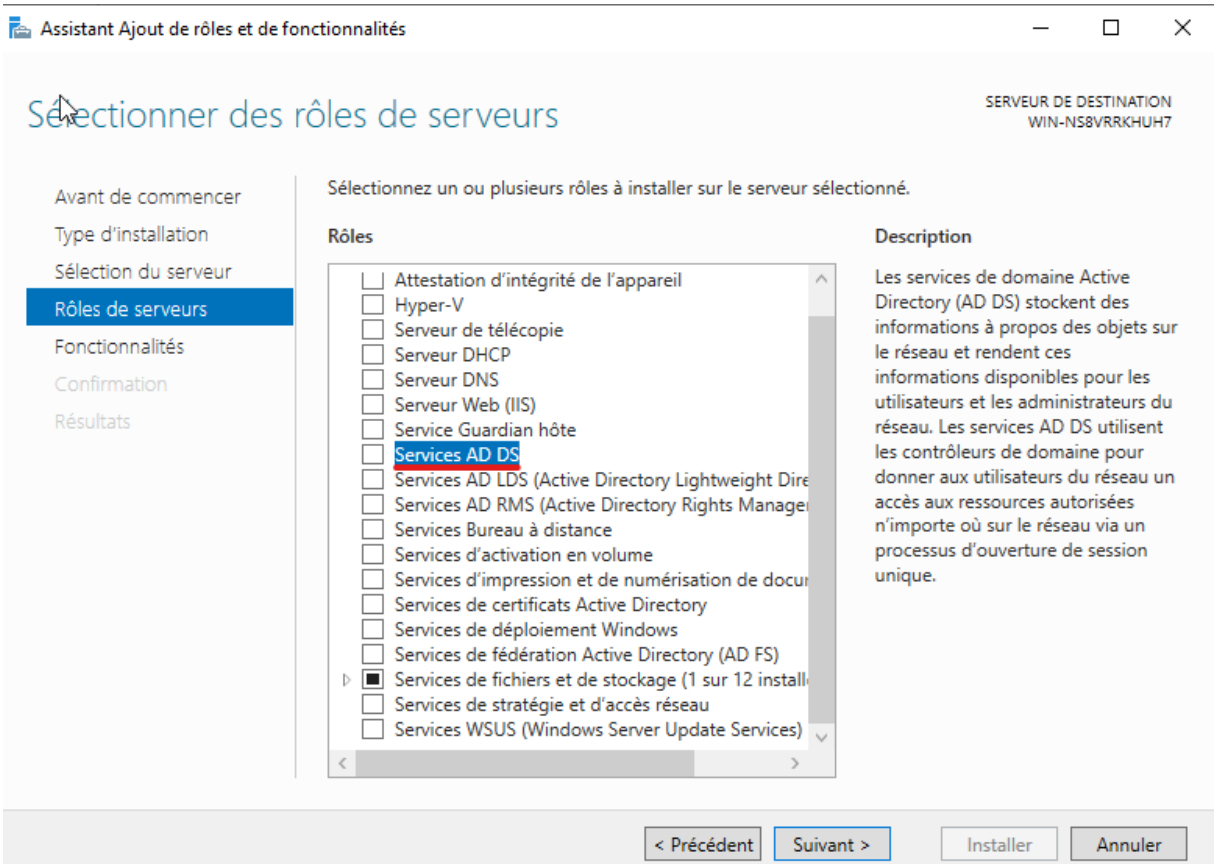
Nous cliquons sur « Suivant ».

Etape 10



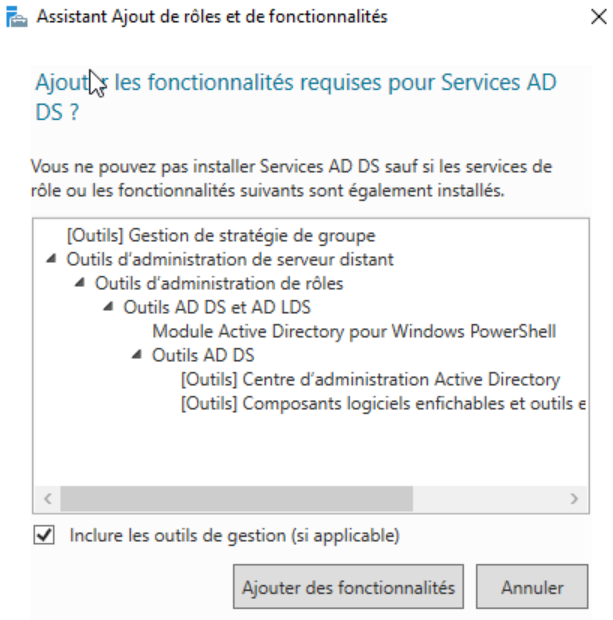
Nous cliquons sur « Suivant ».

Etape 11



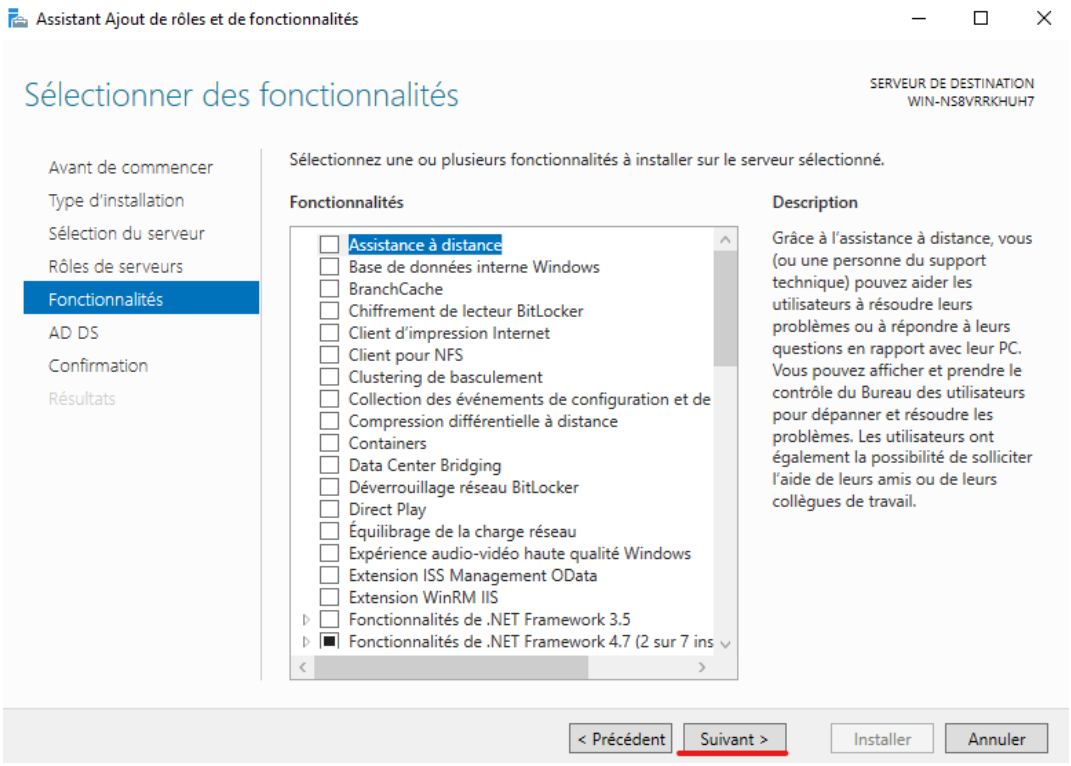
Nous cochons la case « Service AD DS ».

Etape 12



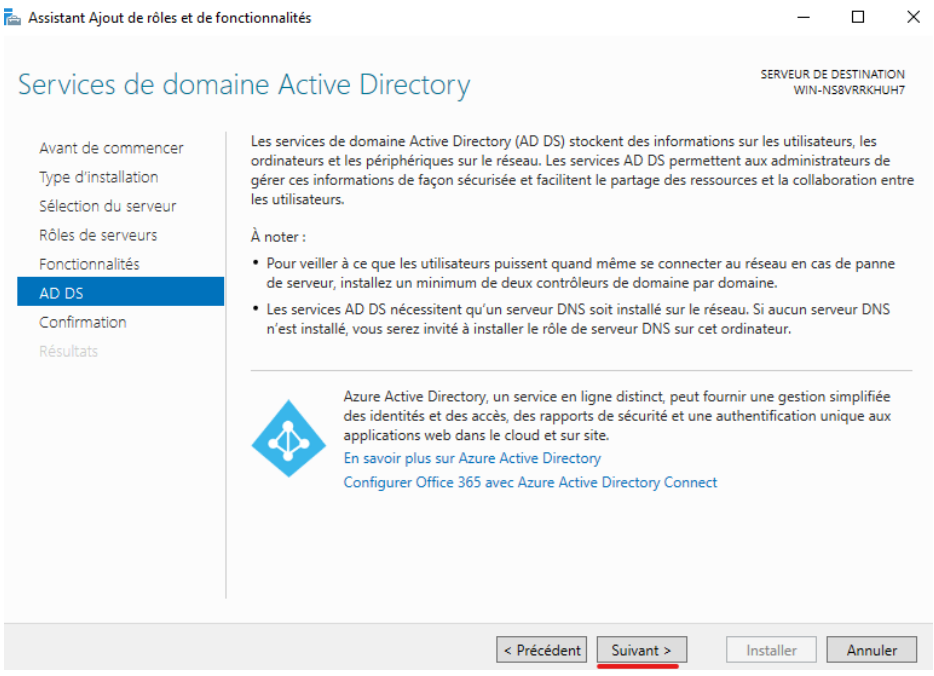
Cette action nous ouvre cette fenêtre récapitulant les fonctionnalités requises pour Services AD DS. Nous cliquons sur « Ajouter des fonctionnalités ».

Etape 13



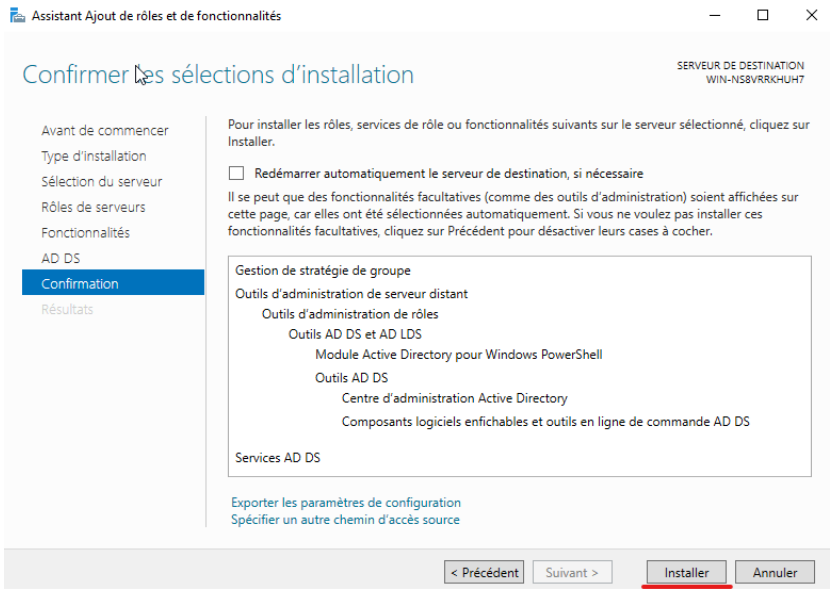
Nous cliquons sur « suivant ».

Etape 14



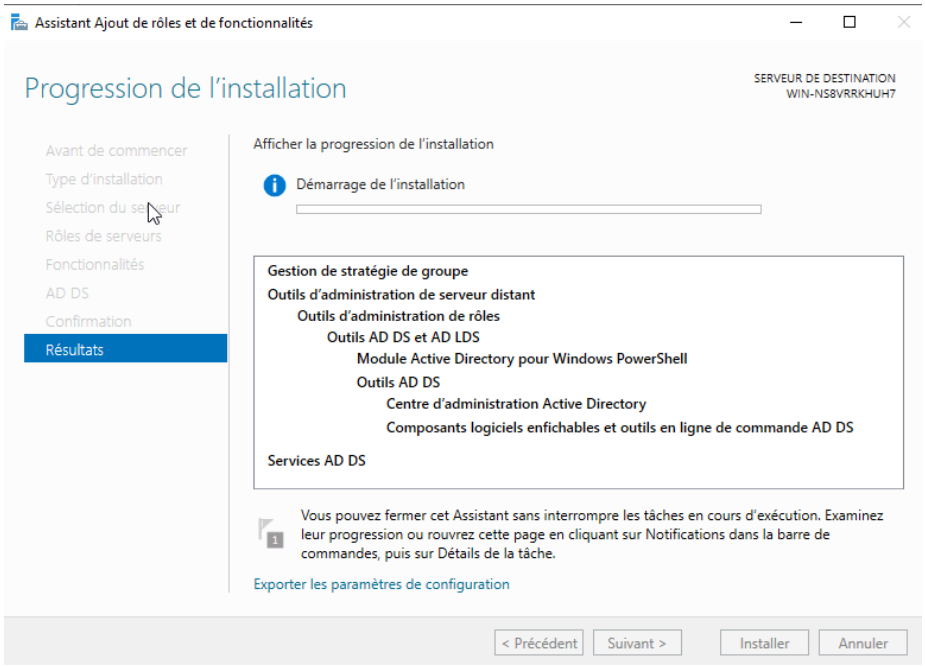
Nous cliquons sur « Suivant ».

Etape 15



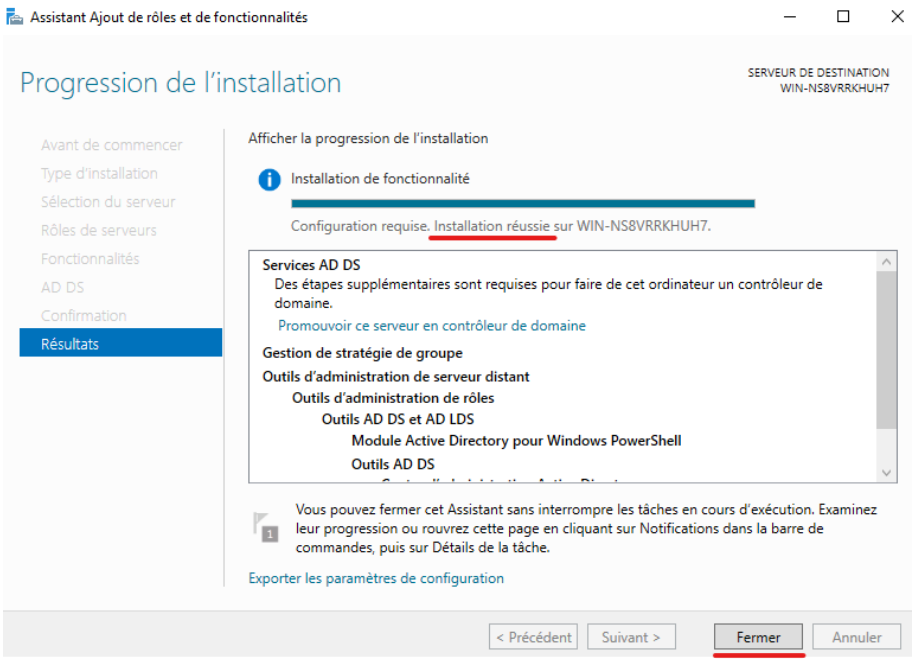
Nous cliquons sur « Installer ».

Etape 16



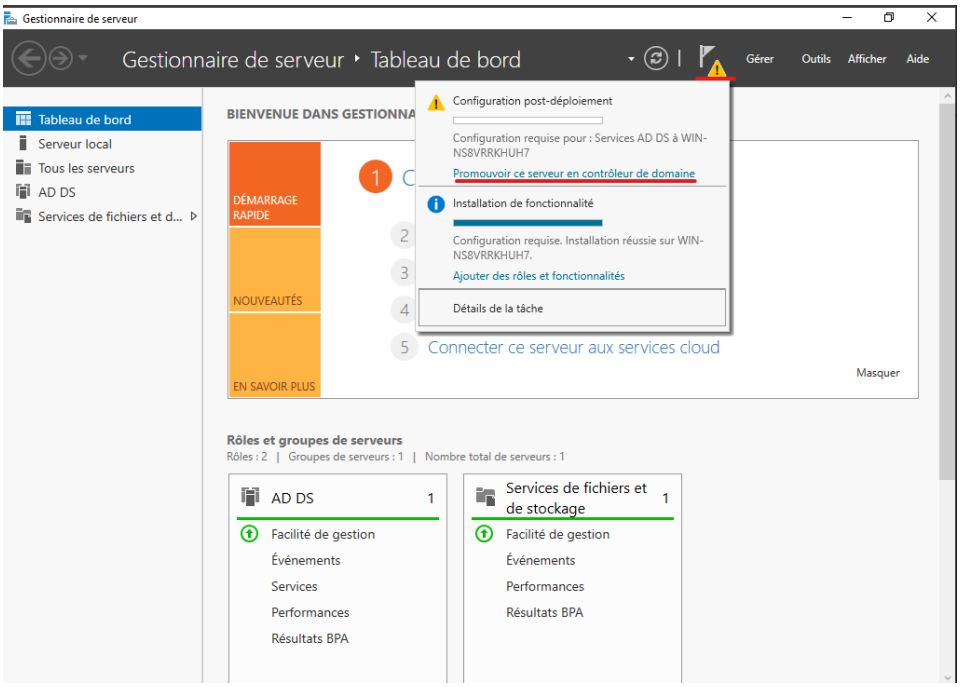
Nous attendons que l'installation finisse.

Etape 17



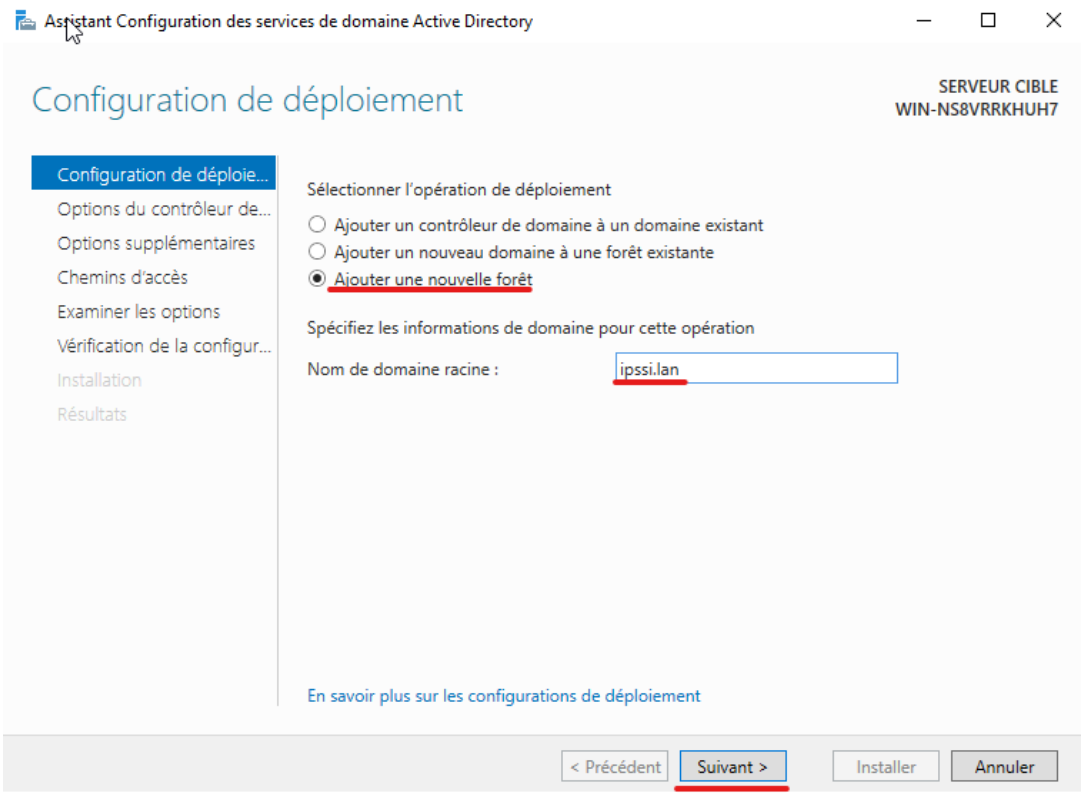
Une fois que l'installation est finie, nous fermons cette page.

Etape 18



Un triangle jaune avec un point d'exclamation apparaît en haut de page, nous cliquons dessus puis sur « Promouvoir ce serveur en contrôleur de domaine ». Cela implique que ce serveur devra vérifier les identifications, traiter les demandes d'authentification, veiller à l'application des stratégies de groupe etc…

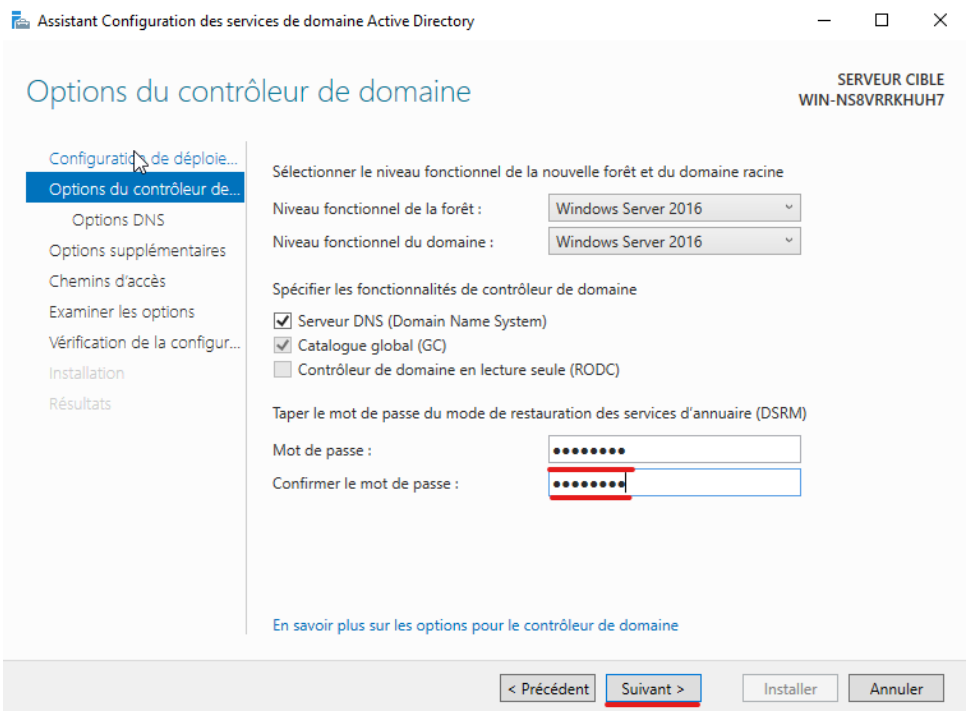
Etape 19



Nous ajoutons une nouvelle forêt, ici ipssi.lan, puis nous cliquons sur « Suivant ».

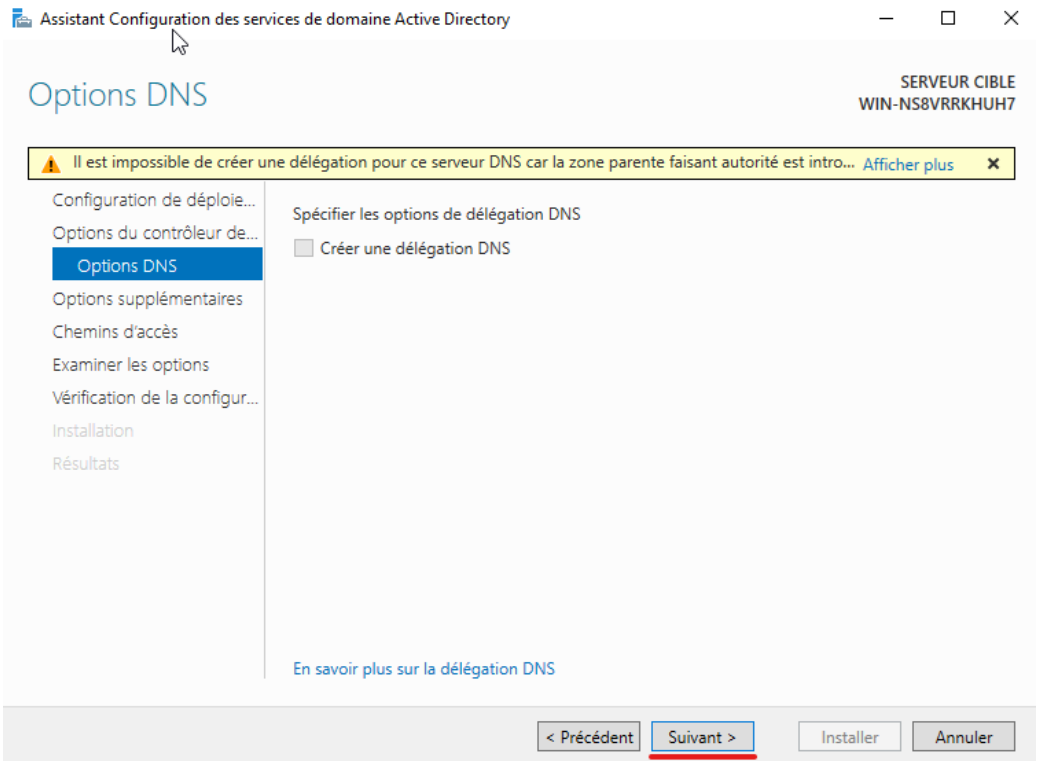
Une forêt se trouve au-dessus des domaines et peut contenir plusieurs domaines. Par exemple pour la forêt ipssi.lan, on peut avoir les domaines etudiant.ipssi.lan ou professeur.ipssi.lan.

Etape 20



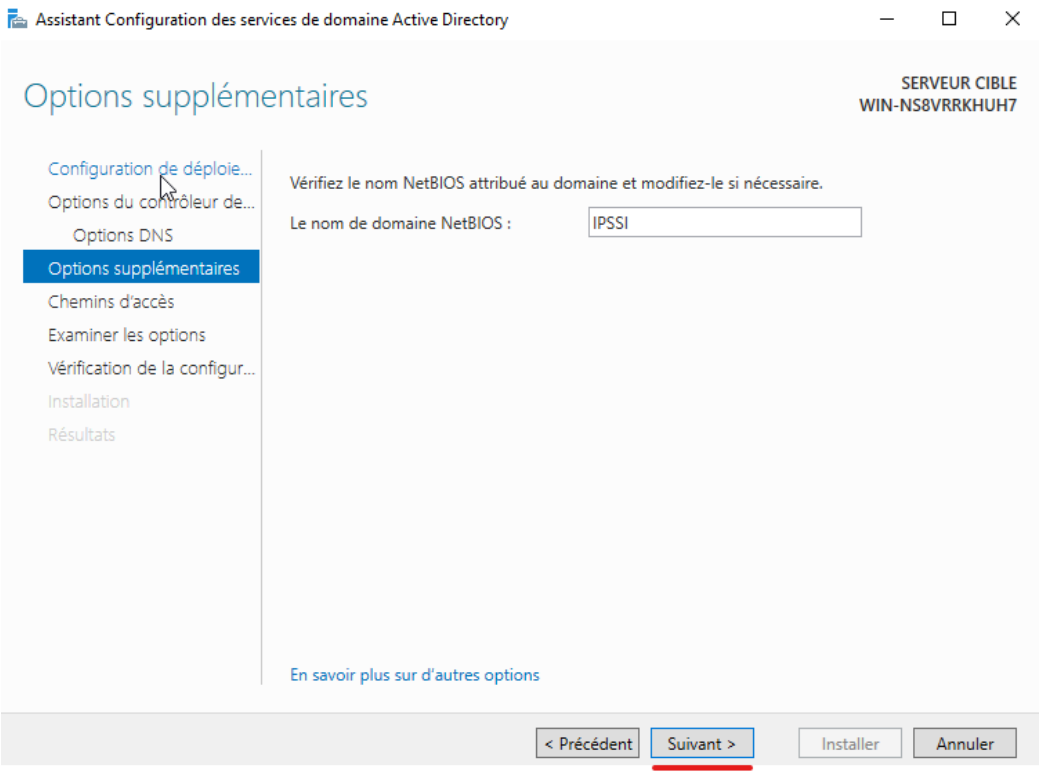
Nous saisissons un mot de passe, puis nous cliquons sur « Suivant ».

Etape 21



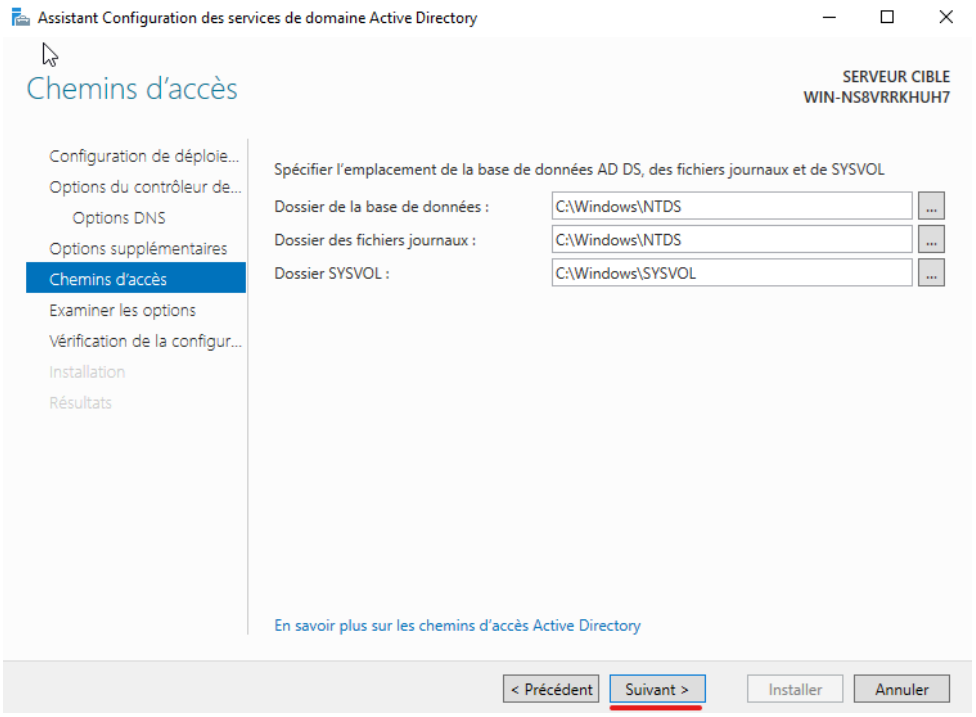
Nous cliquons sur « Suivant ».

Etape 22



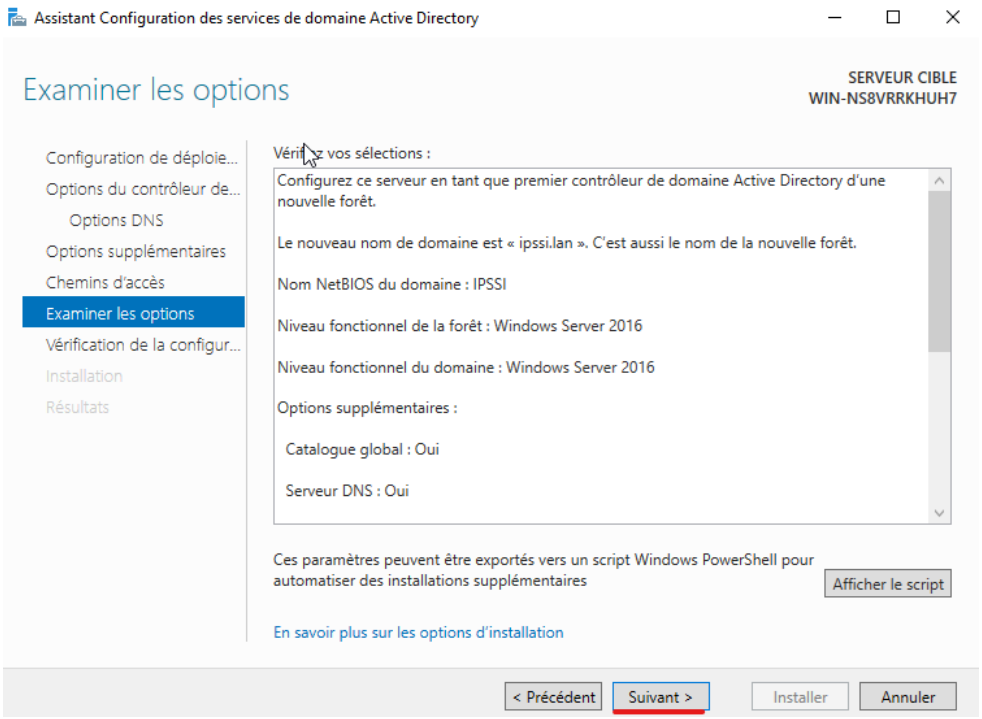
Le nom de domaine NetBIOS s'ajoute automatique, ici IPSSI. Nous cliquons sur « Suivant ».

Etape 23



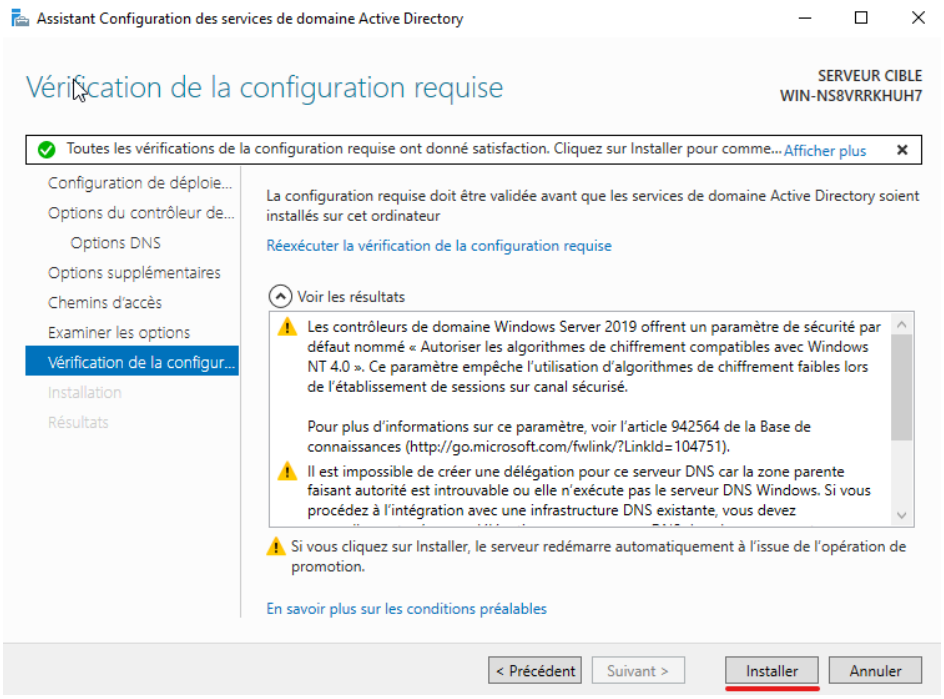
Nous cliquons sur « Suivant ».

Etape 24



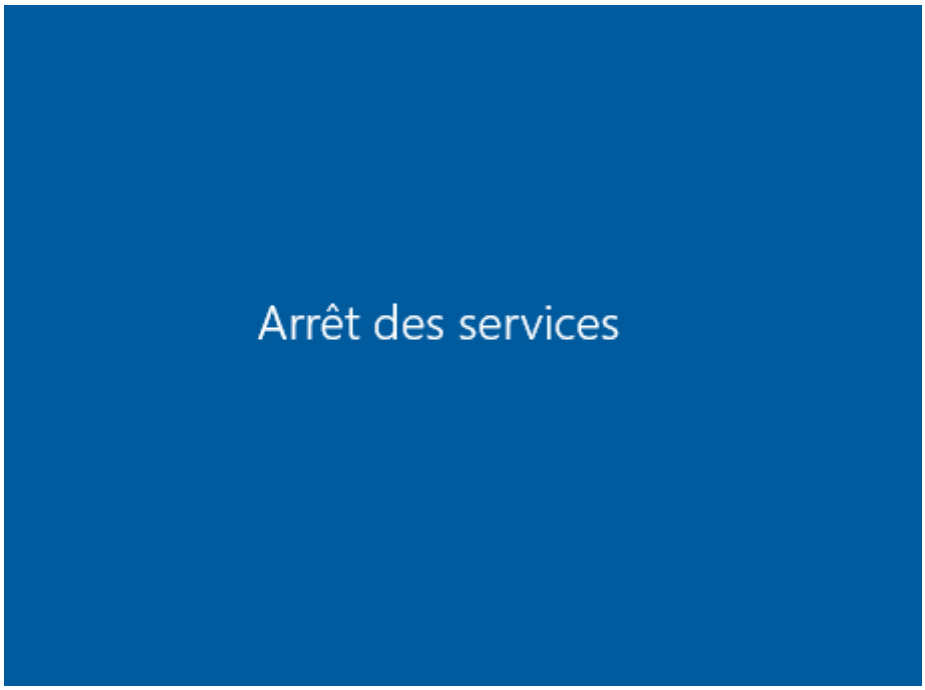
Nous cliquons sur « Suivant ».

Etape 25



Nous cliquons sur « Installer ».

Etape 26

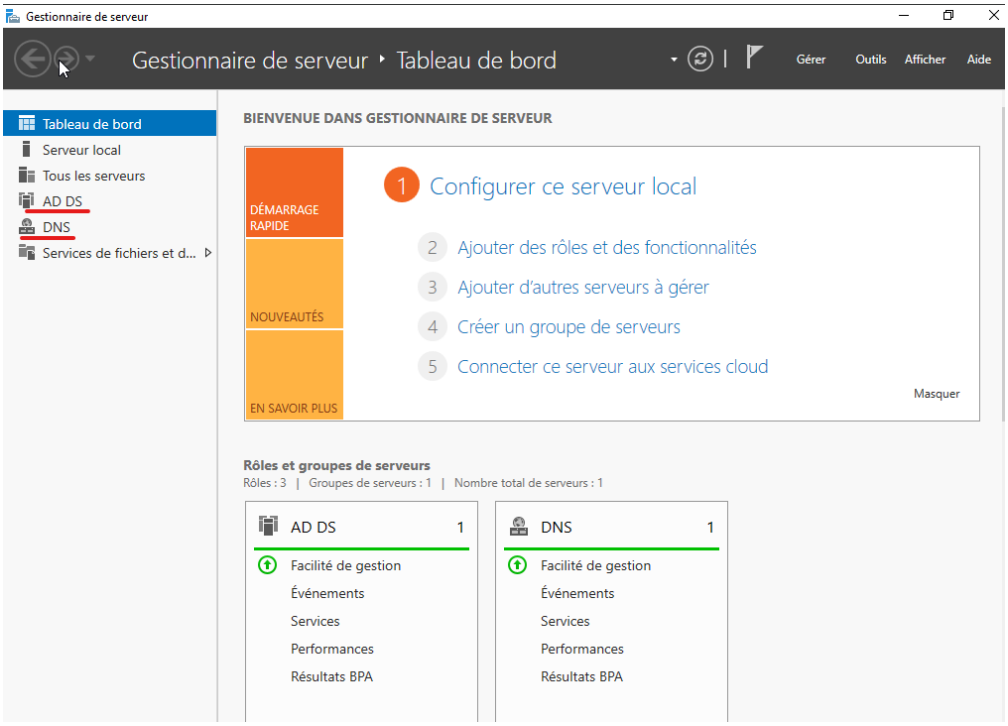


Une fois l'installation terminée, WS19 redémarre.

Etape 27

Nous observons que le domaine est bien créé avec la racine IPSSI\.

Etape 28

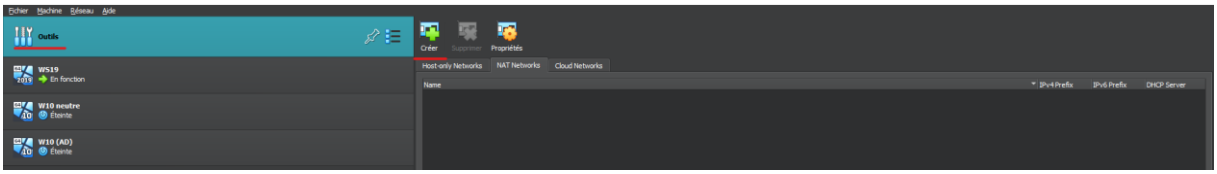


Nous observons deux nouveaux onglets : AD DS et DNS (Domain Name Service).

b) Rejoindre le domaine

Maintenant que le domaine ipssi.lan est créé, nous allons voir comment un autre poste peut rejoindre ce domaine.

Etape 1



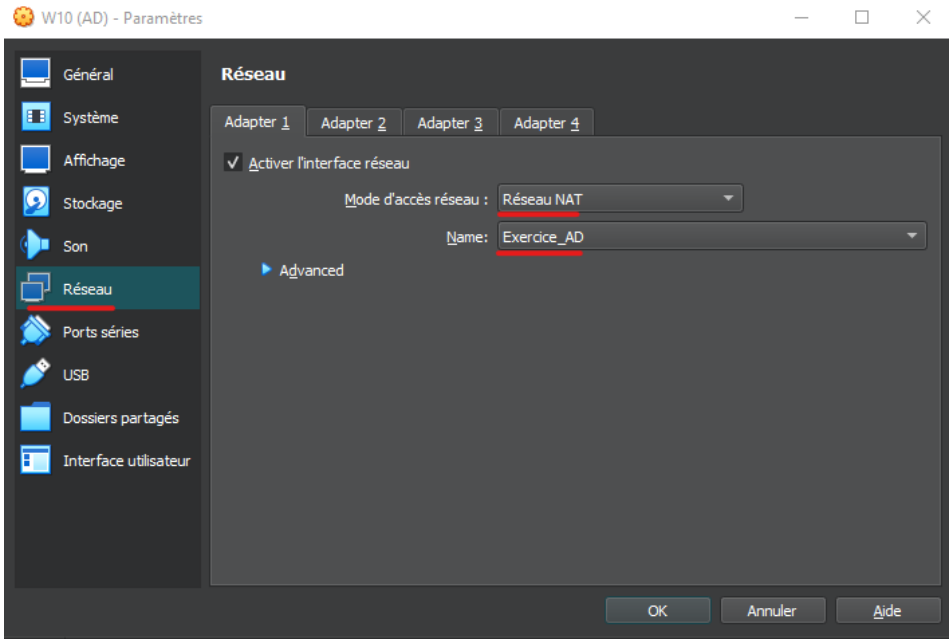
Dans notre cas, nous utilisons l'hyperviseur de type 2 « VirtualBox ». Pour créer un réseau virtuel, nous nous rendons dans « Outils » puis une fois dans « Nat Networks », nous cliquons sur créer.

Etape 2

Cet onglet apparaît en bas de page, nous remplissons les informations comme ci-dessus.

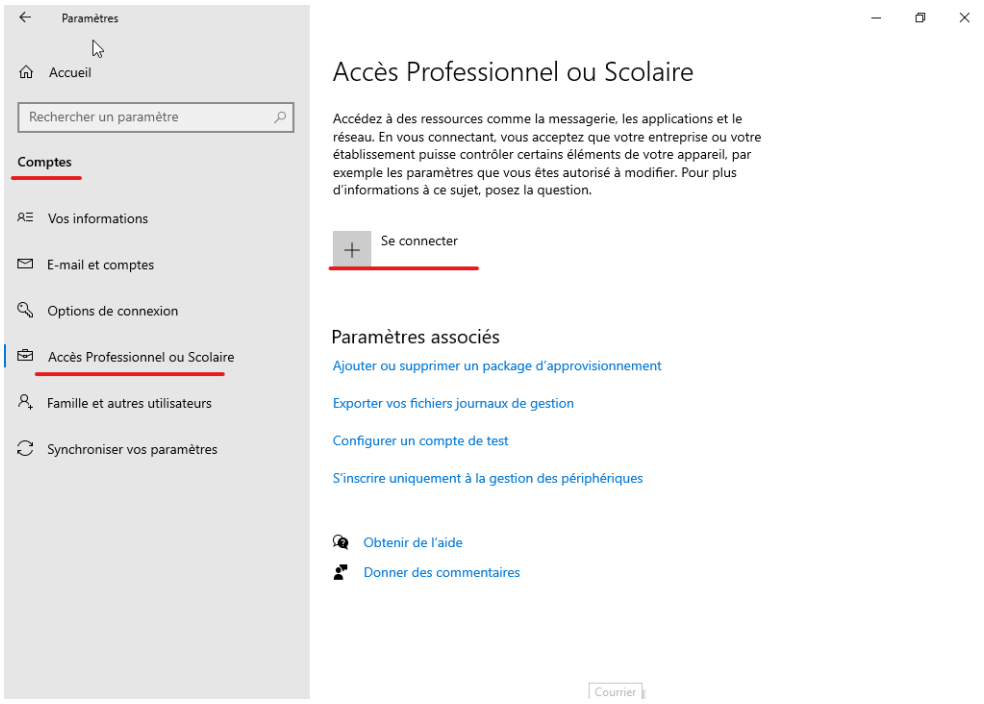
Il est important de désactiver le DHCP car chaque poste doit avoir une adresse IP statique pour le bon déroulement de ce TP.

Etape 3



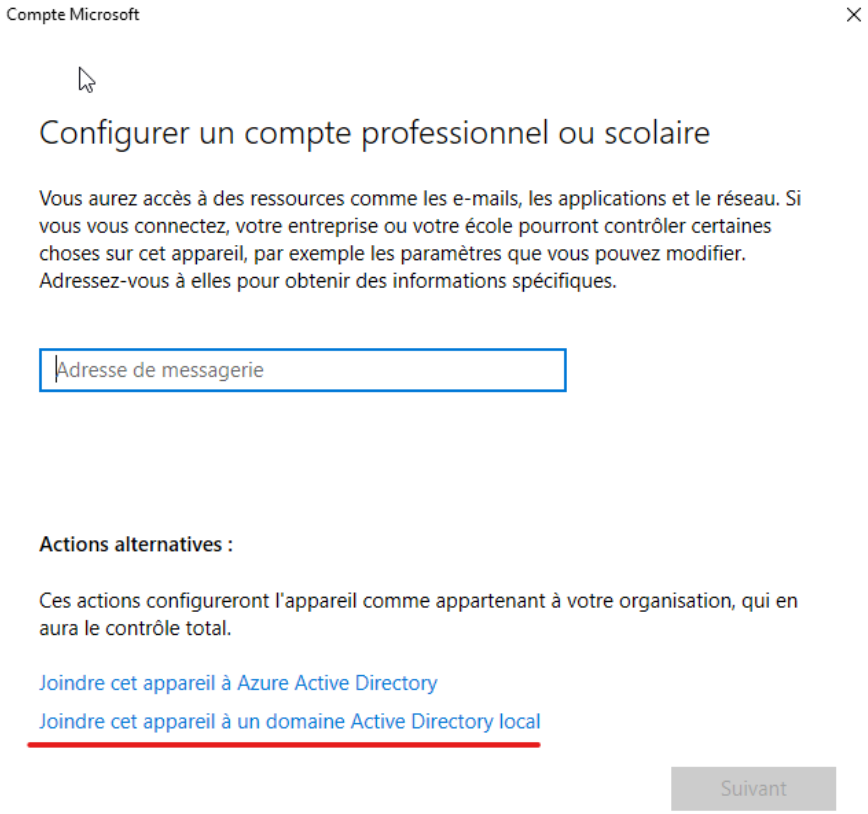
Ensuite chaque VM doit se trouver dans ce réseau. Pour cela, nous nous rendons dans « Réseau » puis nous sélectionnons « Réseau NAT » comme mode d'accès réseau et « Exercice_AD » qui est le réseau que nous venons de créer.

Etape 4



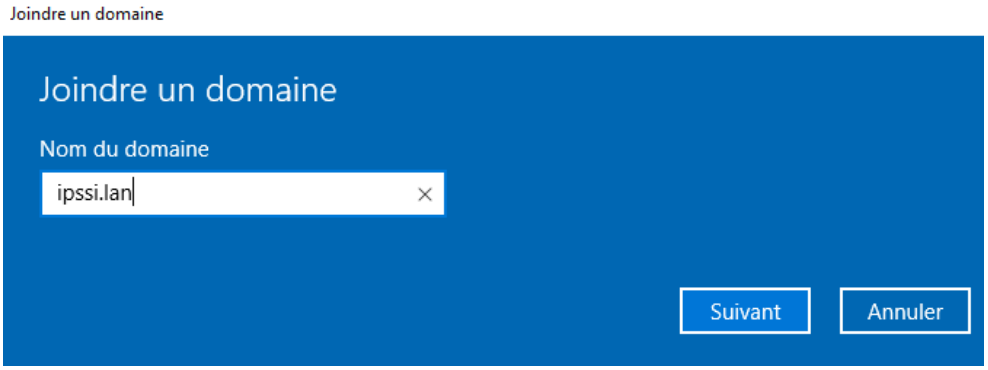
Ensuite, une fois que la MV W10E est démarrée, nous nous rendons dans les paramètres « Comptes », puis « Accès Professionnel ou Scolaire ». Et nous cliquons sur « Se connecter ».

Etape 5



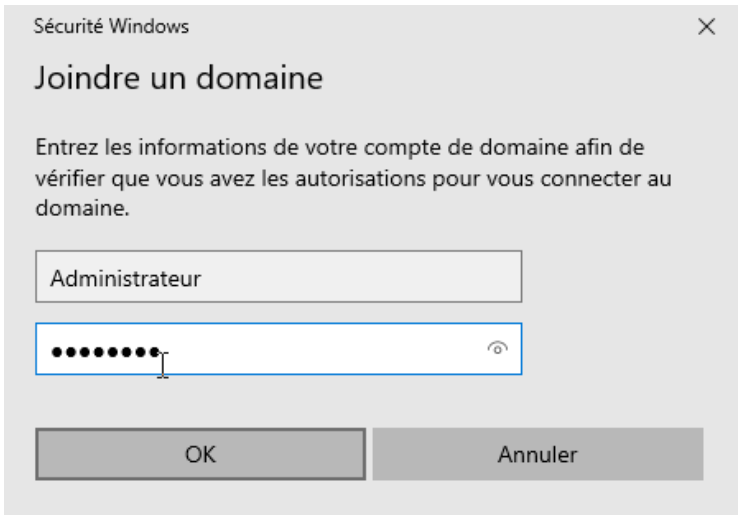
Nous cliquons sur « Joindre cet appareil à un domaine Active Directory local ».

Etape 6



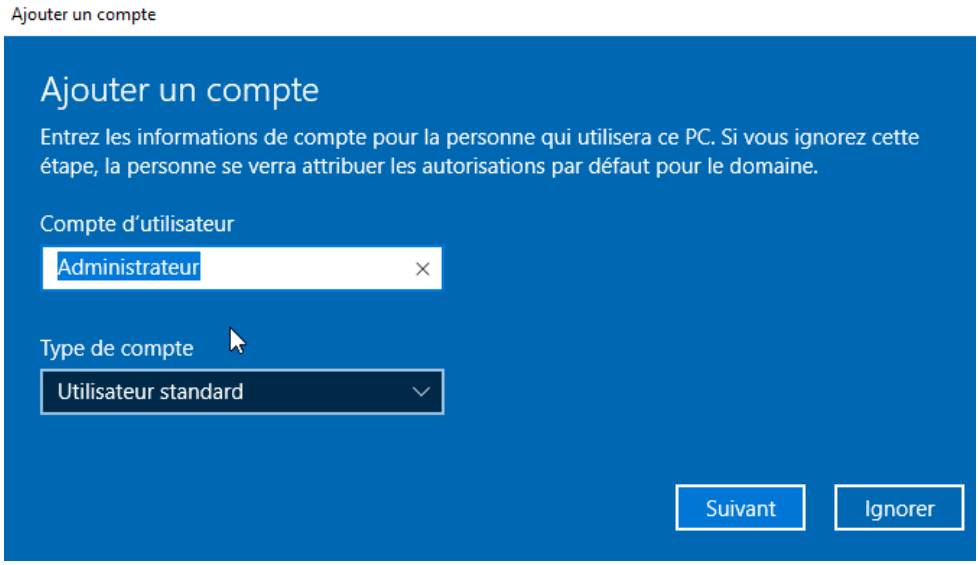
Nous rentrons le nom du domaine, ici ipssi.lan, puis nous cliquons sur « Suivant ».

Etape 7



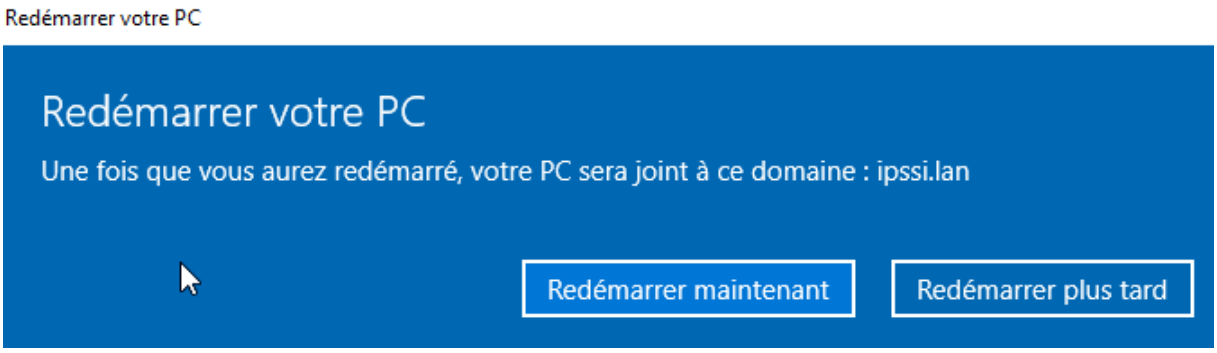
Nous rentrons l'identifiant « Administrateur » et son mot de passe.

Etape 8



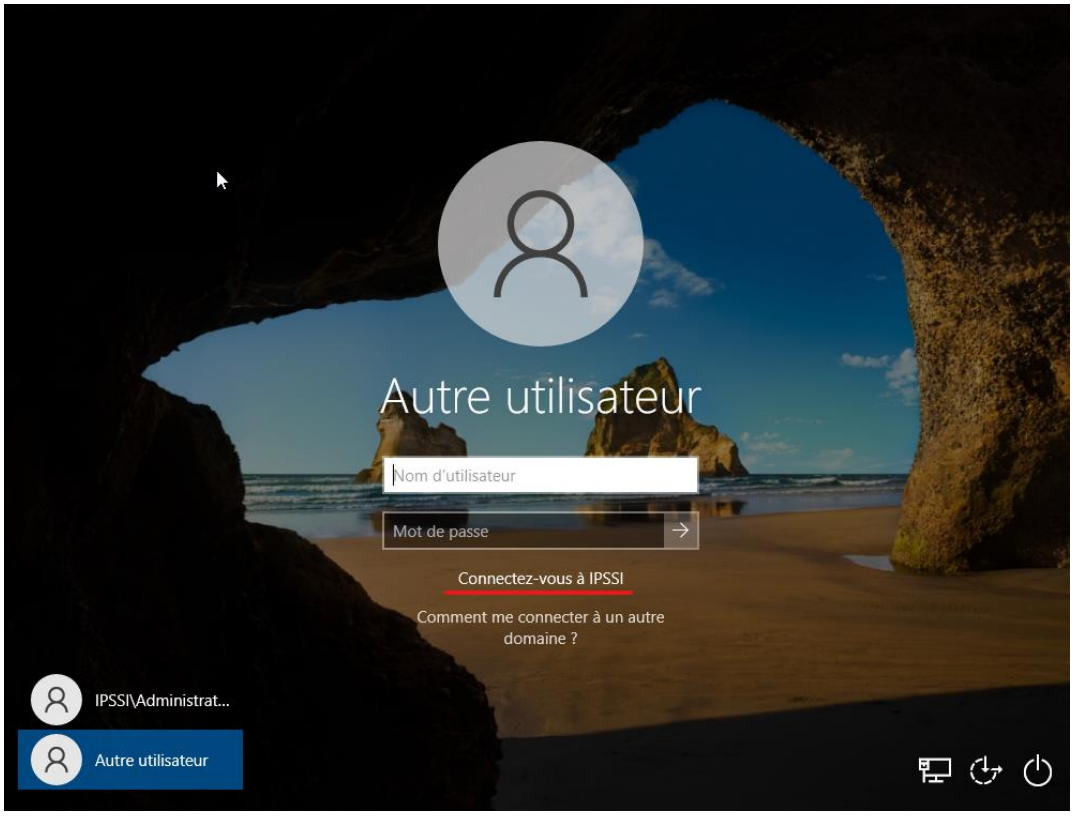
Nous cliquons sur « Suivant ».

Etape 9



Nous cliquons sur « Redémarrer maintenant ».

Etape 10



Nous observons que le poste (W10E) appartient maintenant au domaine IPSSI.

4- UGDLP (User Global DomainLocal Permissions)

Nous allons maintenant créer des salariés fictifs avec chacun ses droits.

Nous allons créer une unité d'organisation (UO) contenant trois techniciens (Technicien1, Technicien2 et Technicien3).

Les trois techniciens se trouveront dans le groupe global « Techniciens », et Technicien1 se trouvera également dans le groupe global Responsable_technicien.

Les droits suivront le tableau suivant :

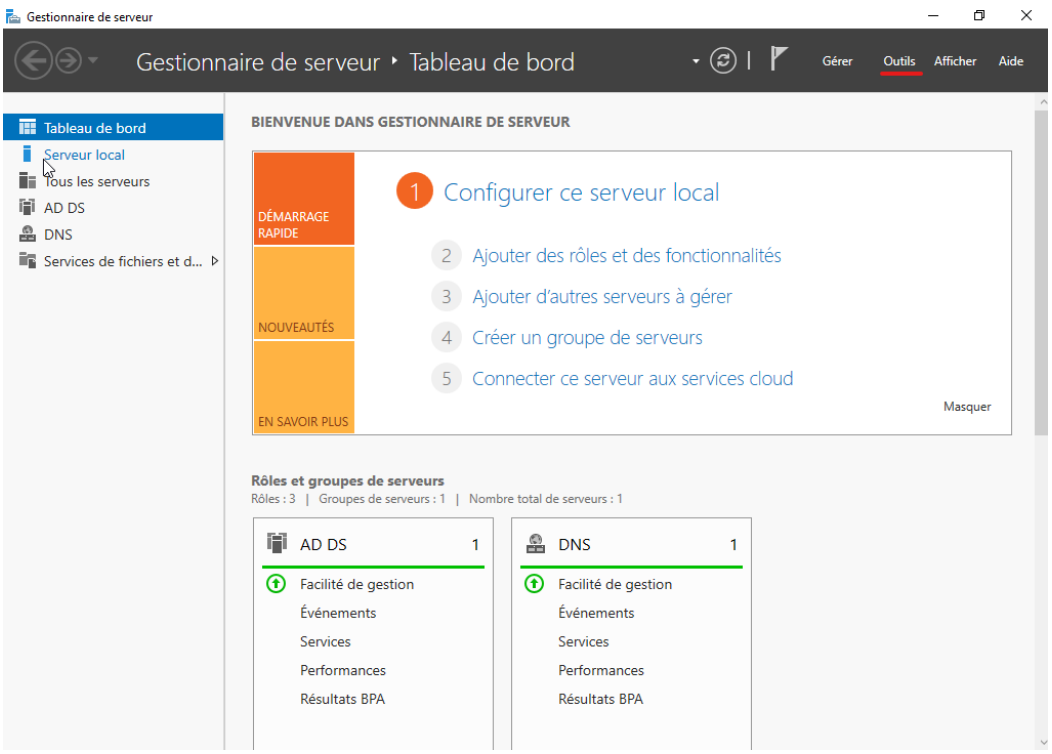
Dossier	Groupe Local	Membre
Technos		Utilisateurs du domaine
Contrats	DL-CT-Contrats	Responsable_technicien
	DL-LS-Contrats	Techniciens
Drivers	DL-CT-Drivers	Techniciens
	DL-LS-Drivers	
Docs	DL-CT-Docs	Techniciens
	DL-LS-Docs	
Logiciels	DL-CT-Logiciels	Techniciens
	DL-LS-Logiciels	Utilisateurs du domaine

(LS : lecture seule, CT : contrôle total)

a) Unité d'organisation « Techniciens »

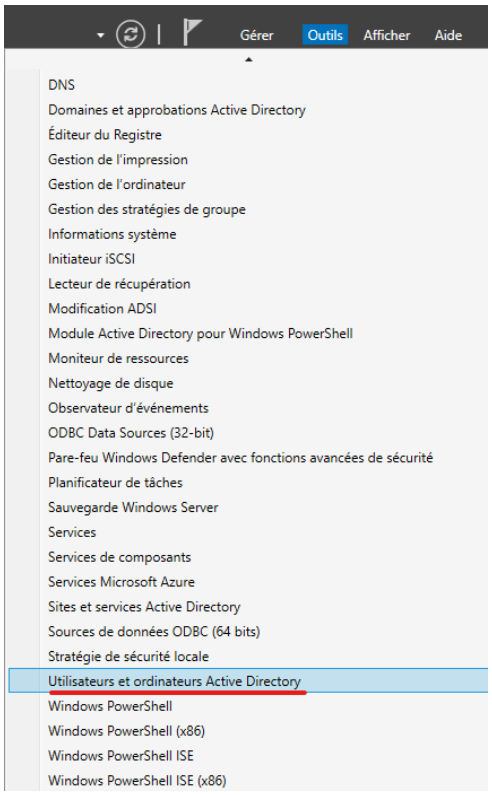
a. Création de l'Unité d'organisation

Etape 1



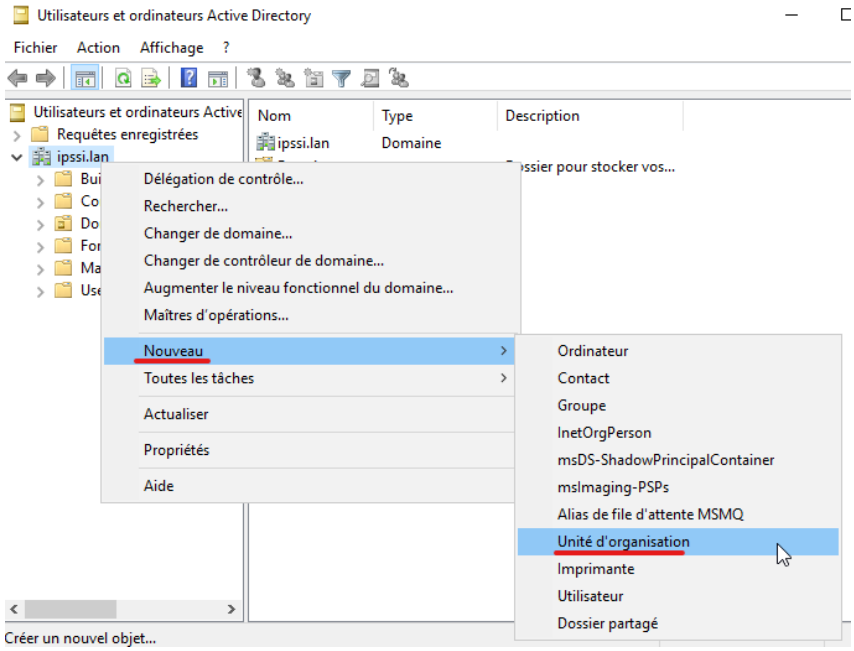
Nous nous rendons dans l'onglet « Outils ».

Etape 2



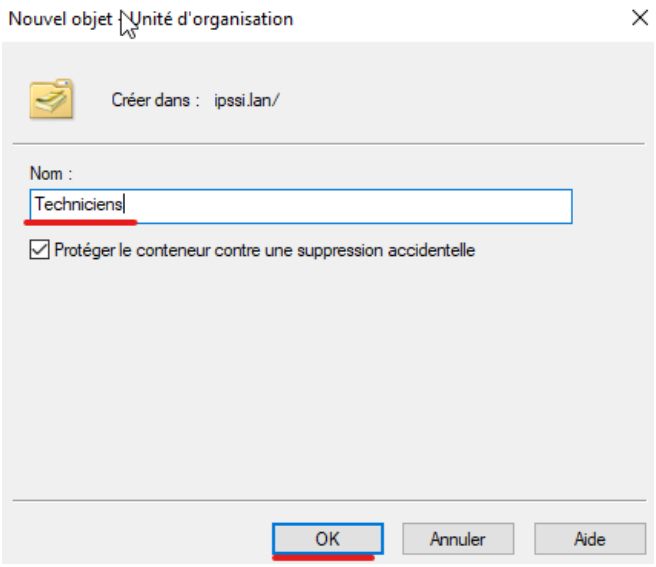
Nous cliquons sur « Utilisateurs et ordinateurs Active Directory ».

Etape 2



Nous faisons un clic droit sur la forêt « ipssi.lan », puis nous cliquons sur « Unité d'organisation » (UO) qui se trouve dans « Nouveau ».

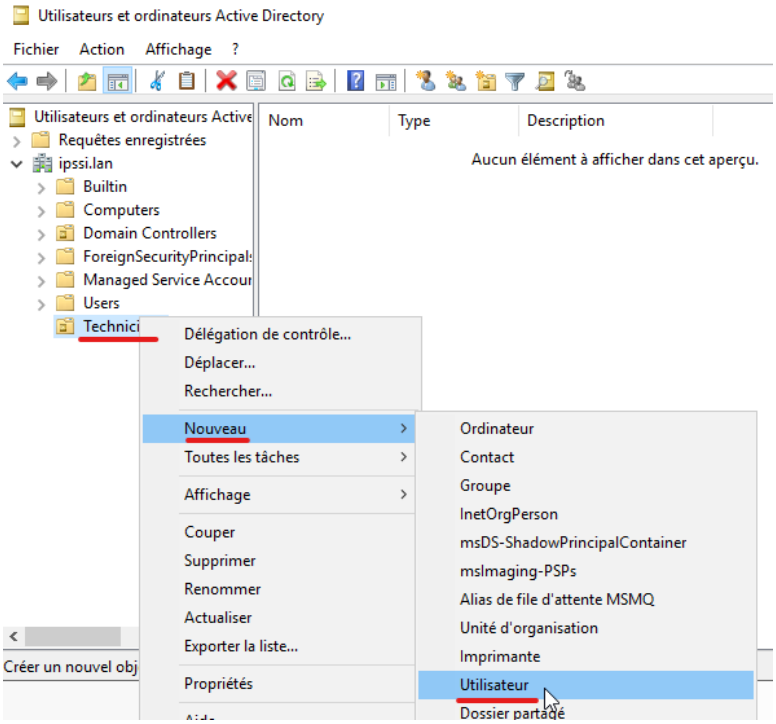
Etape 3



Nous nommons cette nouvelle UO « Techniciens » puis nous cliquons sur « Ok ».

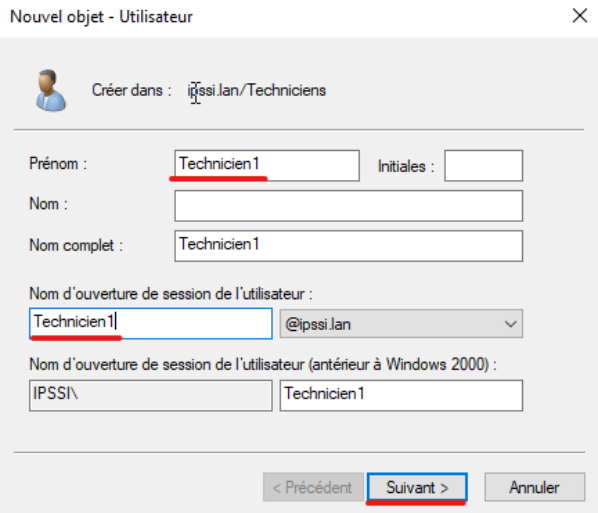
b. Création des utilisateurs

Etape 1



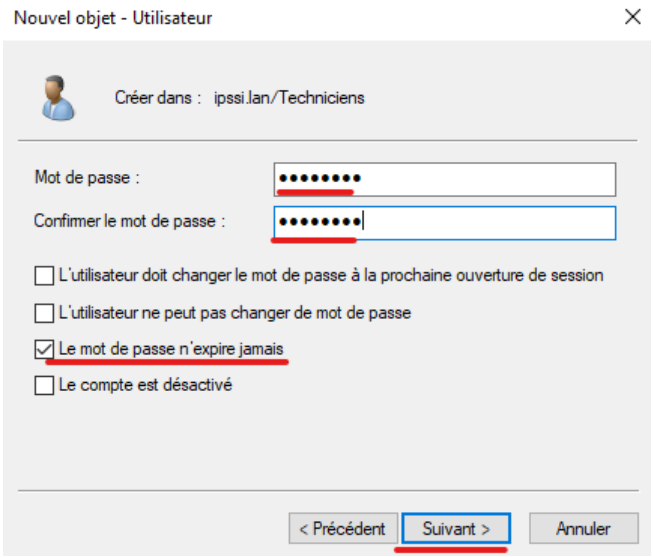
Nous faisons un clic droit sur l'UO « techniciens », puis nous cliquons sur « Utilisateur» (UO) qui se trouve dans « Nouveau ».

Etape 2



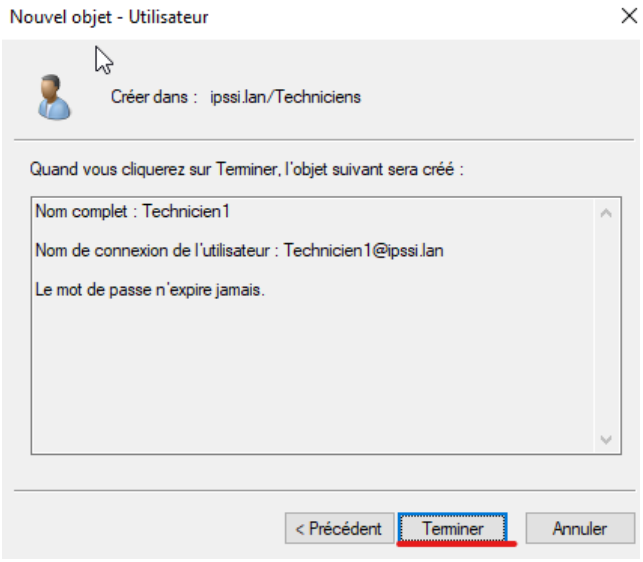
Nous créons le profil de notre premier utilisateur Technicien1, puis nous cliquons sur « Suivant ».

Etape 3



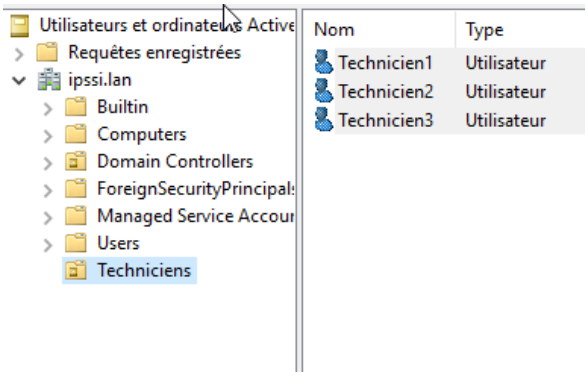
Nous lui attribuons un mot de passe qui n'expirera jamais car il s'agit d'une simulation. Il est fortement conseillé de cocher la case « L'utilisateur doit changer son mot de passe à la prochaine ouverture de session ».

Etape 4



Nous cliquons sur « Terminer ».

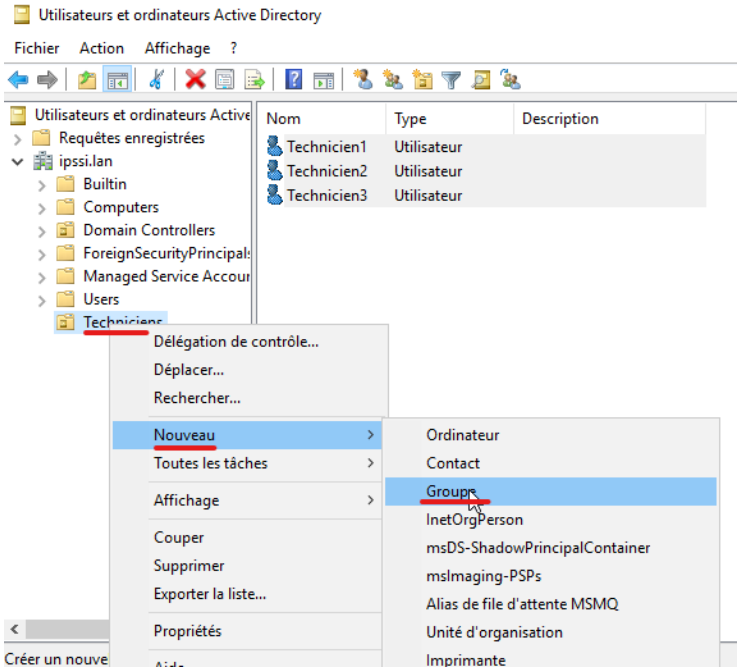
Etape 5



Nous répétons cette opération pour les deux autres techniciens.

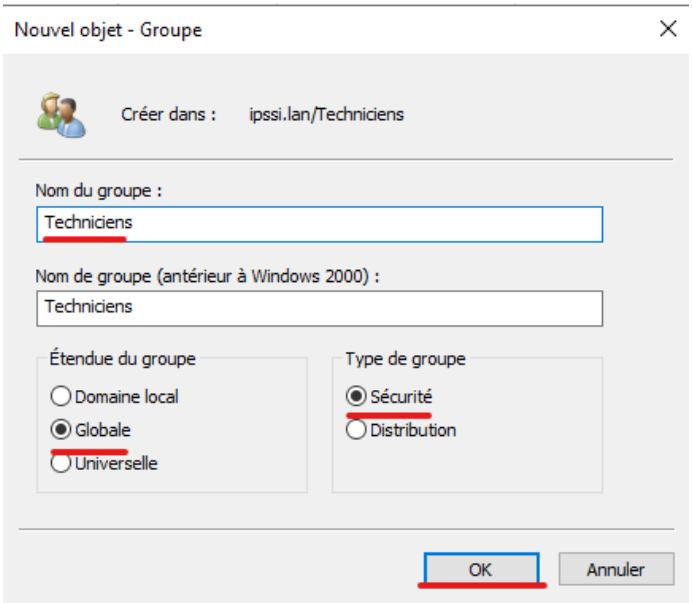
c. Création des groupes globaux

Etape 1



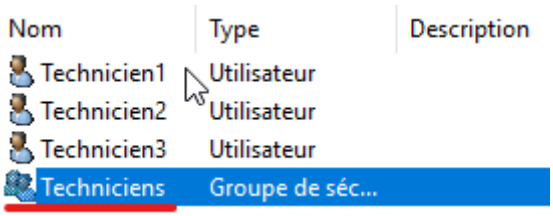
Nous faisons un clic droit sur l'UO « techniciens », puis nous cliquons sur « Groupe» qui se trouve dans « Nouveau ».

Etape 2



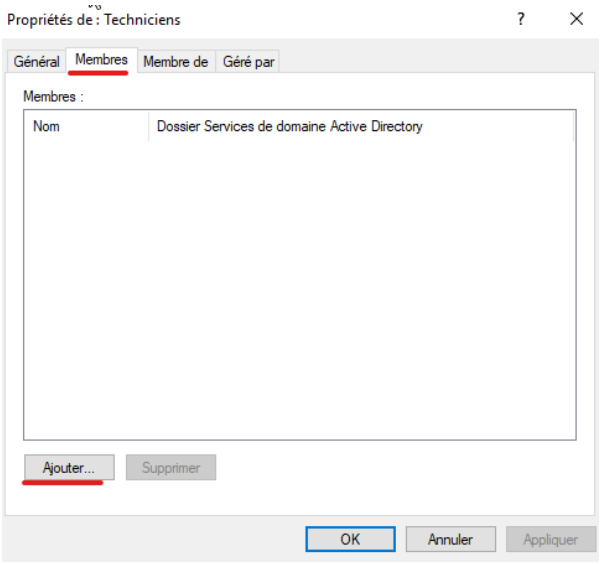
Nous nommons ce groupe « Techniciens », nous le définissons comme étant un groupe global. Nous cliquons sur « ok ».

Etape 3



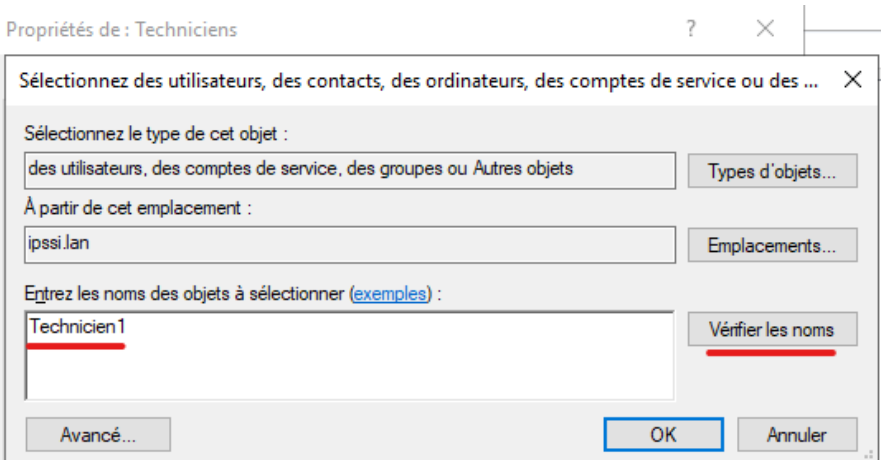
Le groupe « Techniciens » est bien créé, nous doube-cliquons dessus.

Etape 4



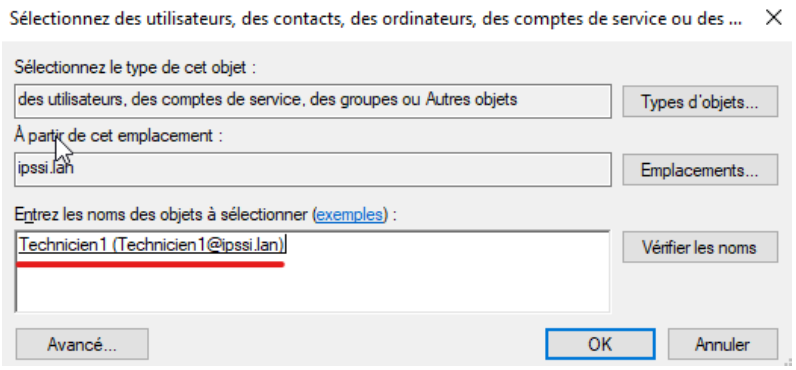
Nous nous rendons dans l'onglet « Membres » et nous cliquons sur « Ajouter… ».

Etape 5



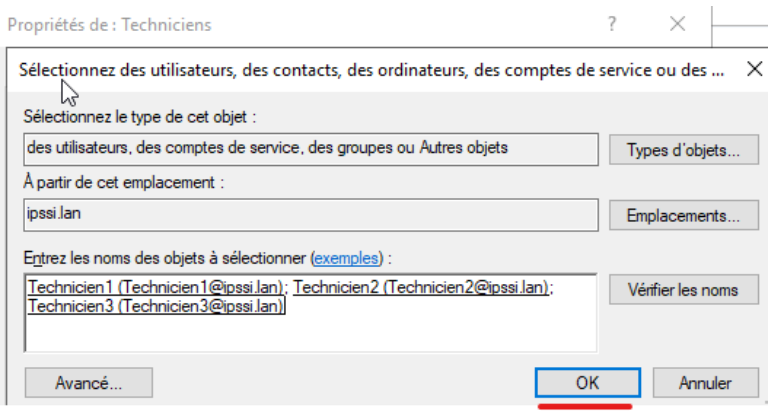
Nous écrivons « Technicien1 » et nous vérifions le nom.

Etape 6



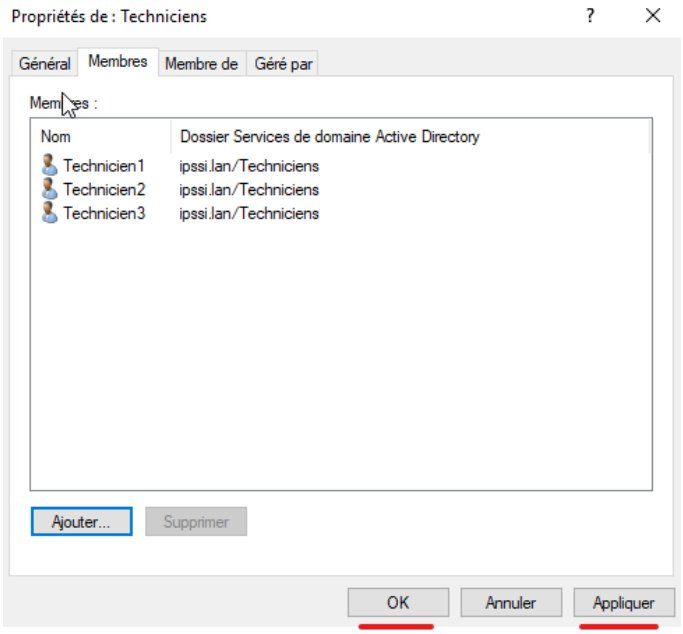
Lorsque le nom est validé, il est souligné.

Etape 7



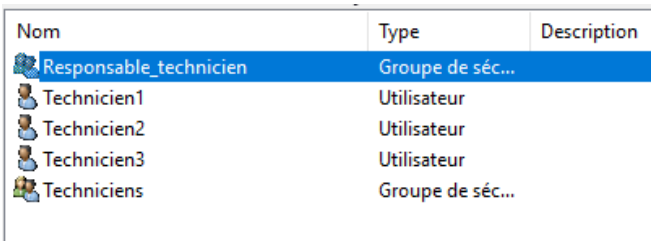
Nous répétons la même opération pour les deux autres techniciens, puis nous cliquons sur « Ok ».

Etape 8



Nous cliquons sur « Ok ».

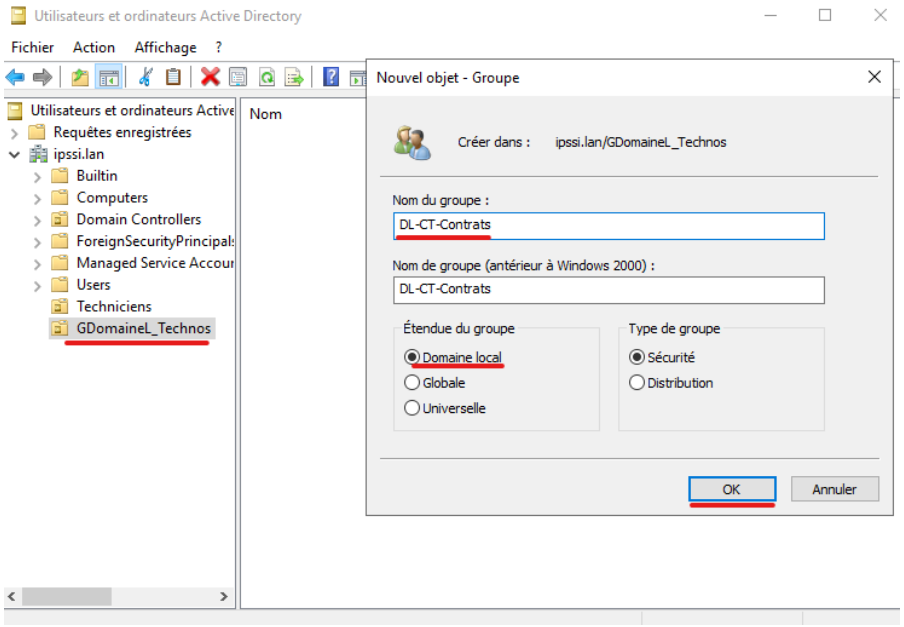
Etape 9



Nous créons également le groupe Responsable_technicien qui contiendra le membre Technicien1.

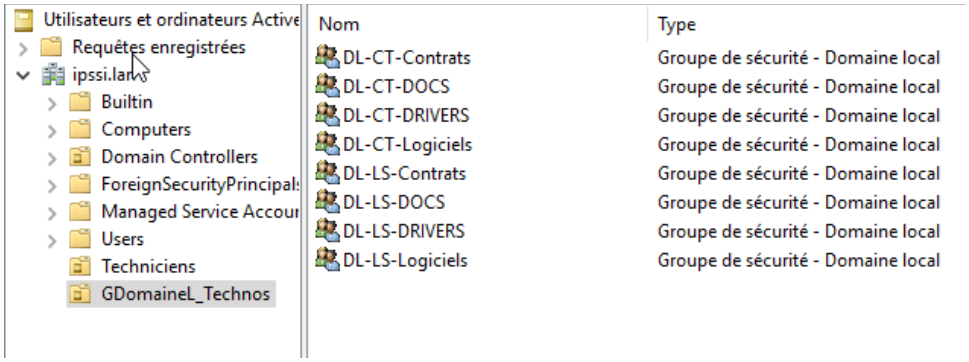
d. Création des groupes locaux

Etape 1



Nous précédons de la même manière que pour les groupes globaux, mais cette fois-ci nous sélectionnons « Groupe local ».

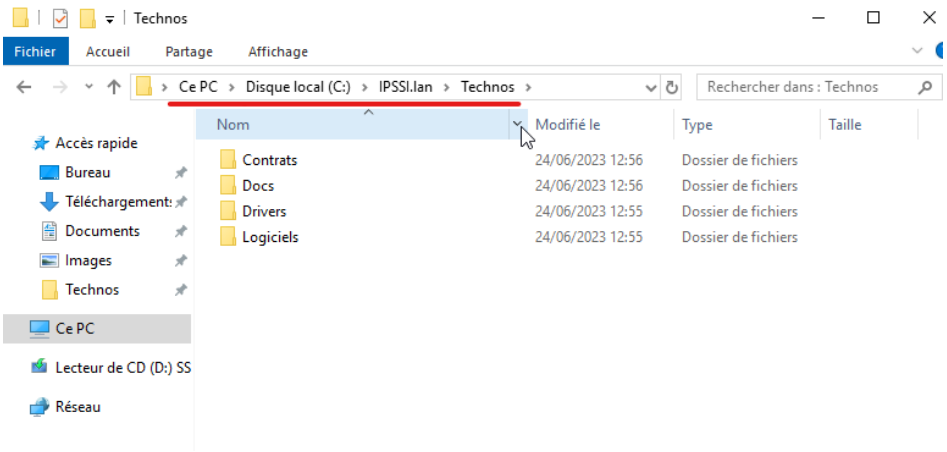
Etape 2



Nous répétons l'opération pour chaque groupe local.

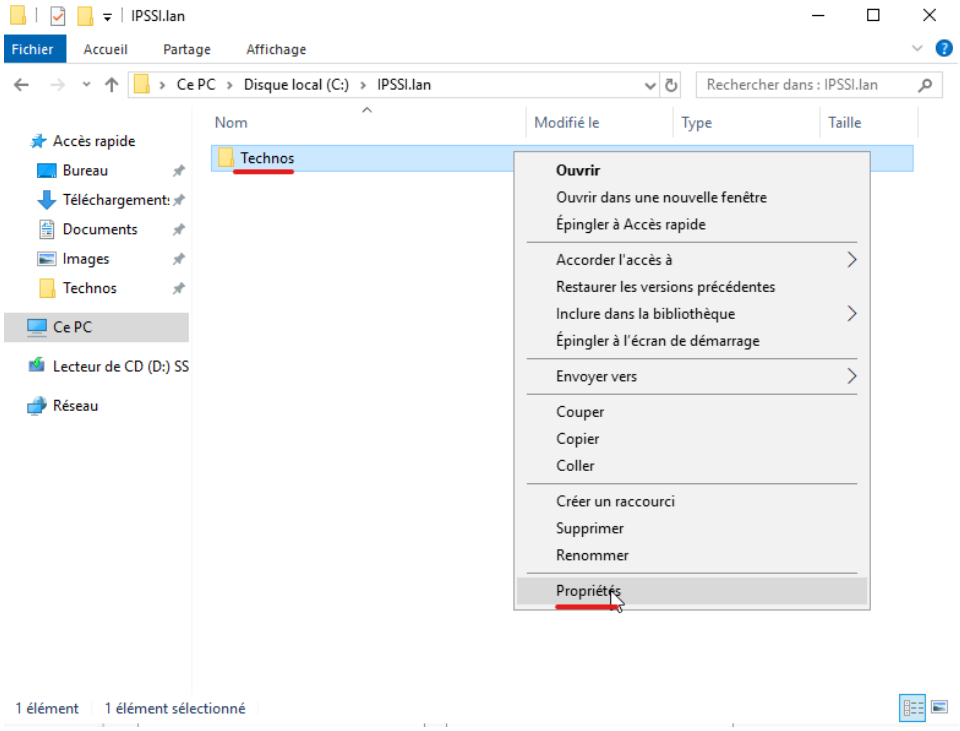
5- Création de fichiers partagés

Etape 1



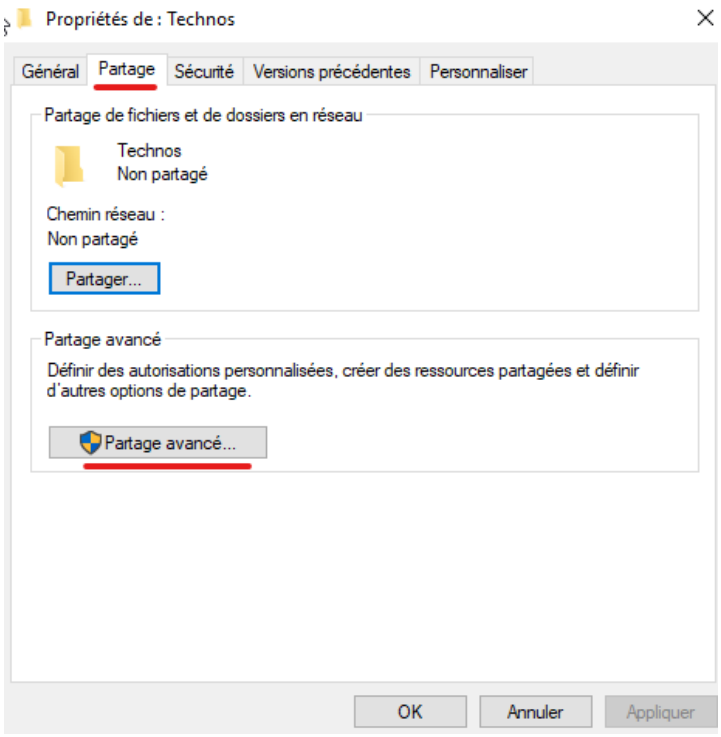
Nous créons ces différents fichiers dans cette arborescence sur WS19.

Etape 2



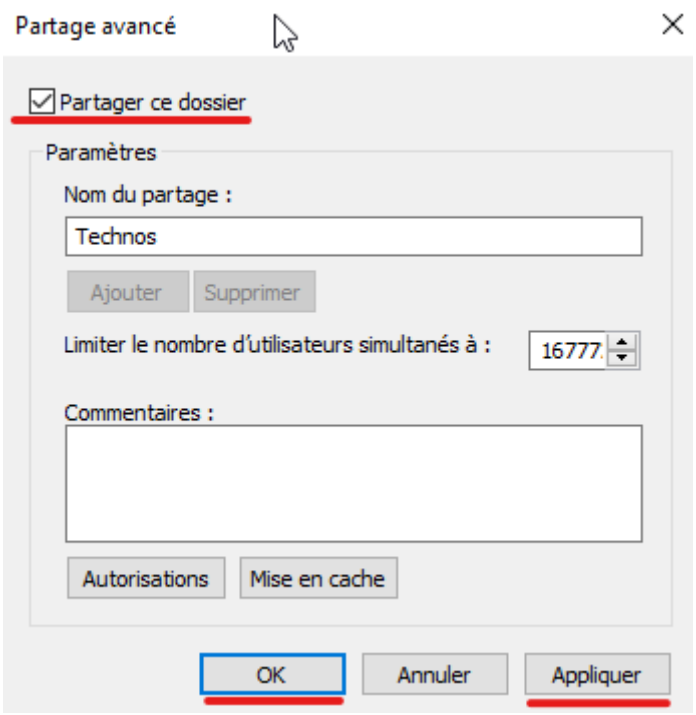
Nous allons dans les propriétés du fichier « Technos ».

Etape 3



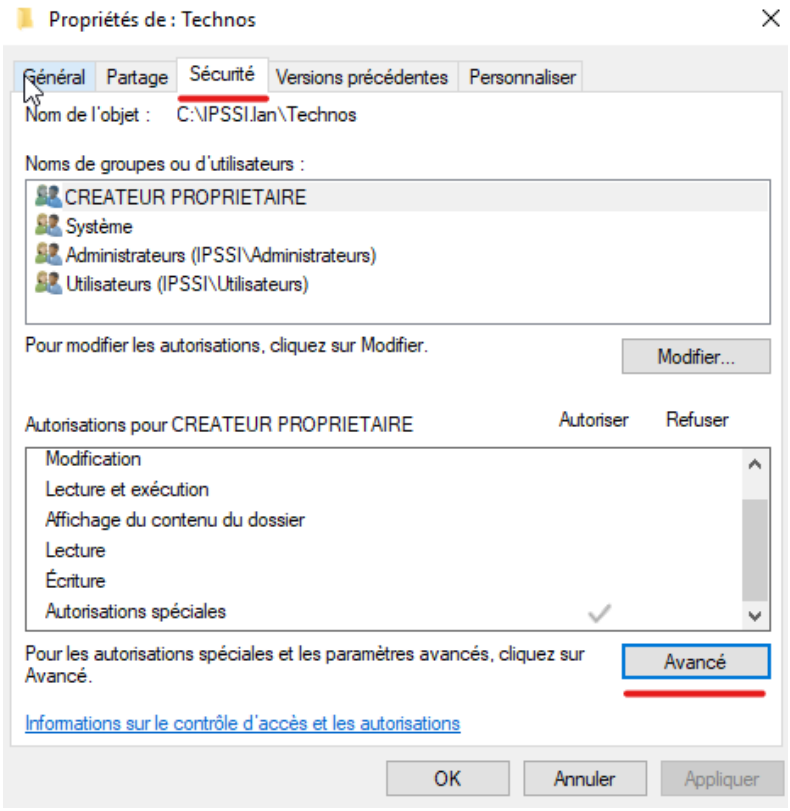
Nous nous rendons dans l'onglet « Partage » puis « Partage avancé… ».

Etape 4



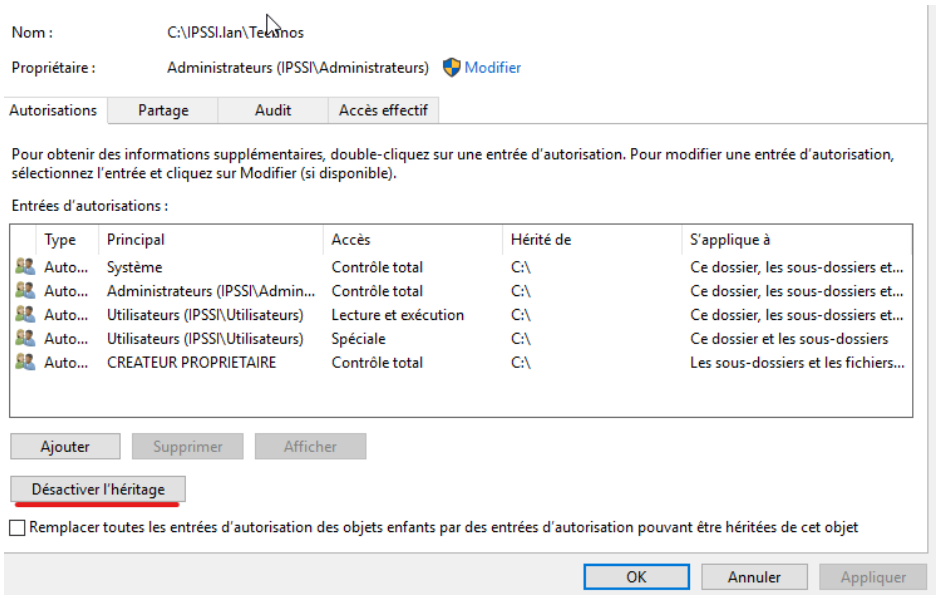
Nous cochons la case « Partager ce dossier » puis nous cliquons sur « ok ».

Etape 5



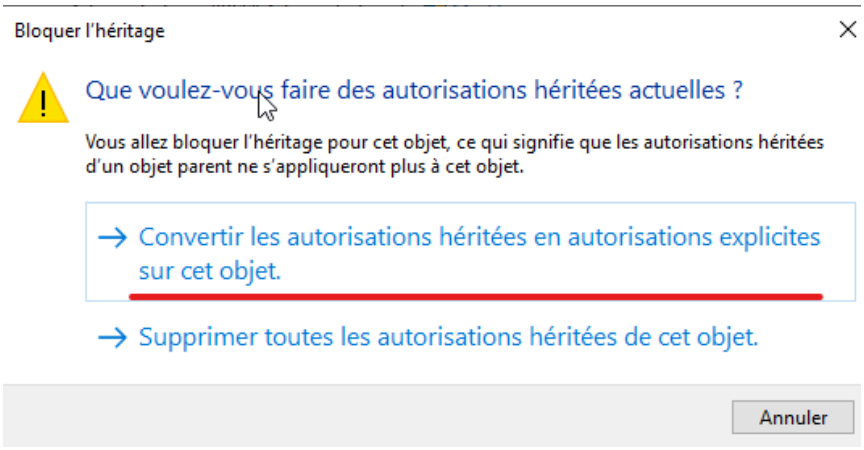
Nous allons ensuite dans l'onglet sécurité, puis « Avancé ».

Etape 6



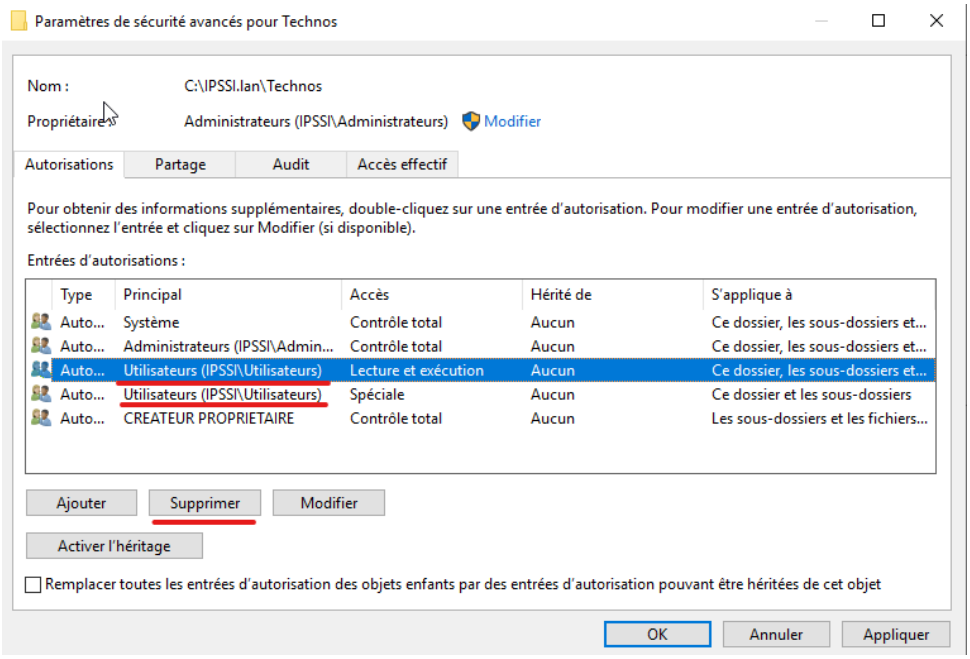
Nous désactivons l'héritage.

Etape 7



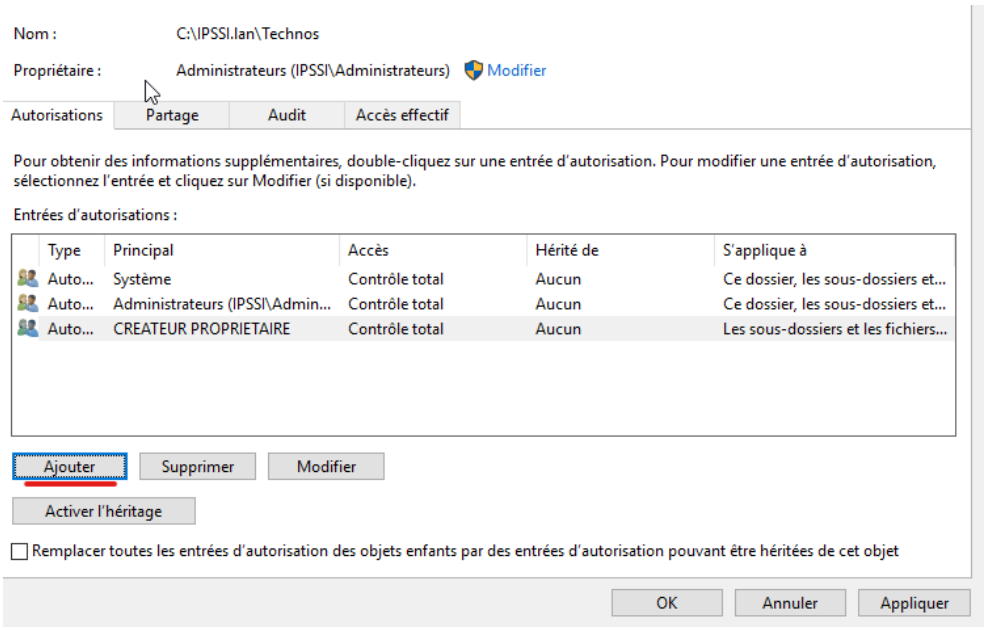
Nous cliquons sur la première option.

Etape 8



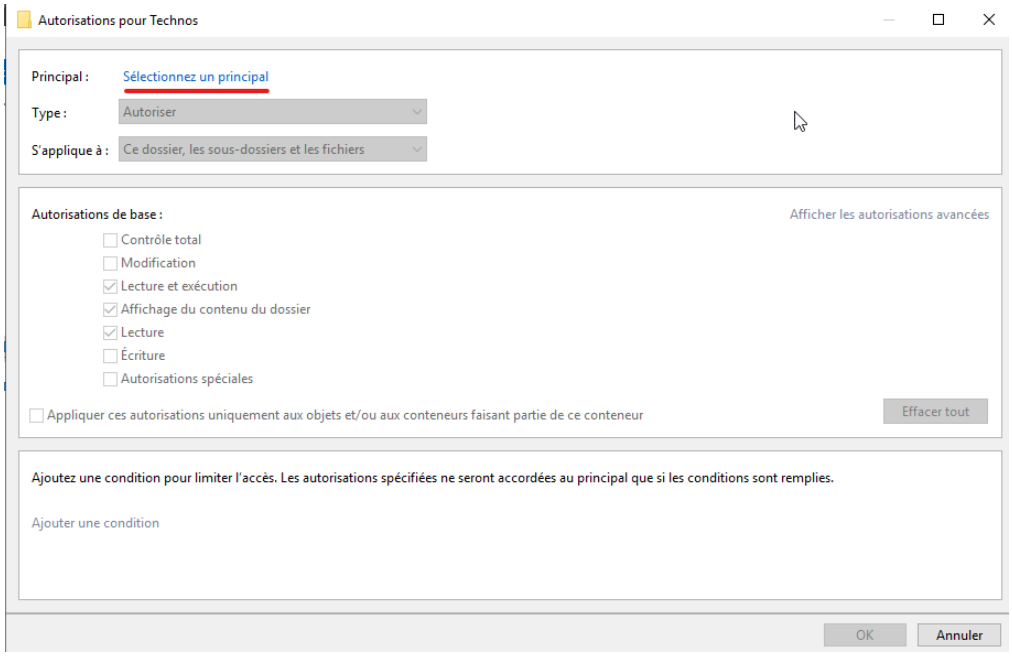
Nous supprimons également les Utilisateurs.

Etape 9



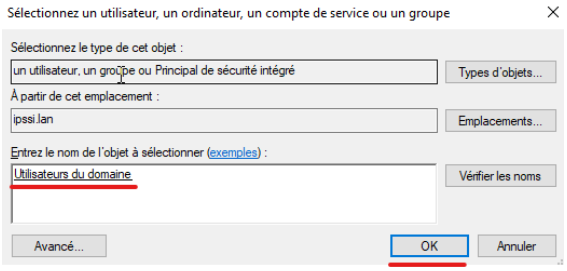
Nous cliquons sur « Ajouter ».

Etape 10



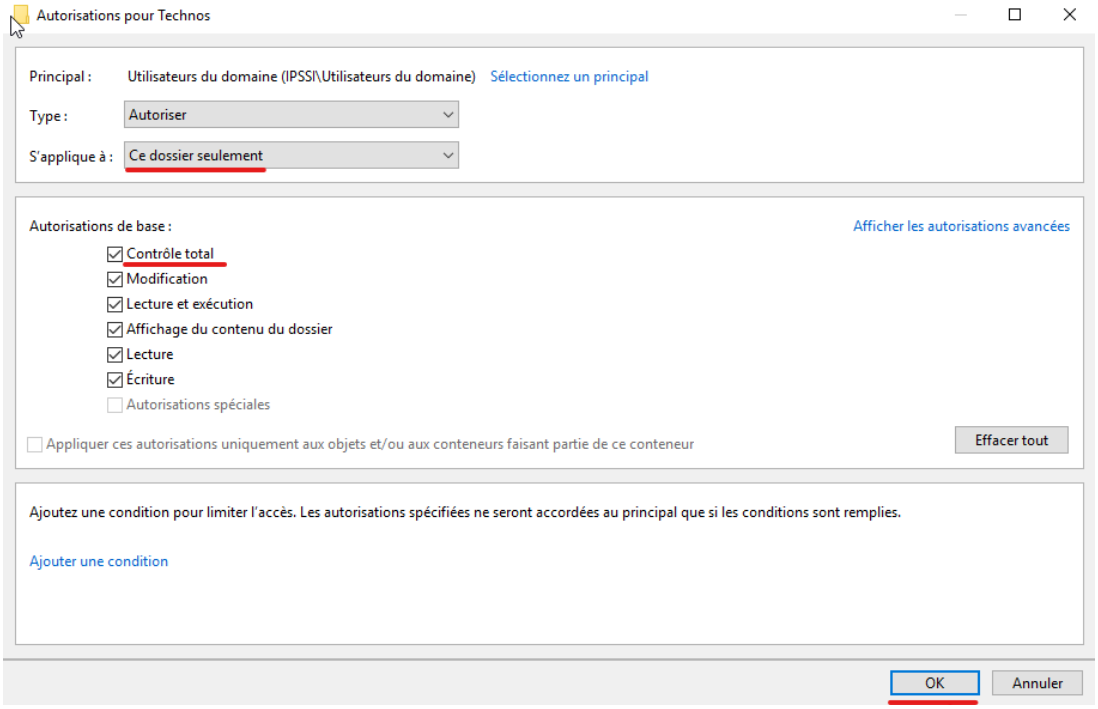
Nous cliquons sur « Sélectionner un principal ».

Etape 11



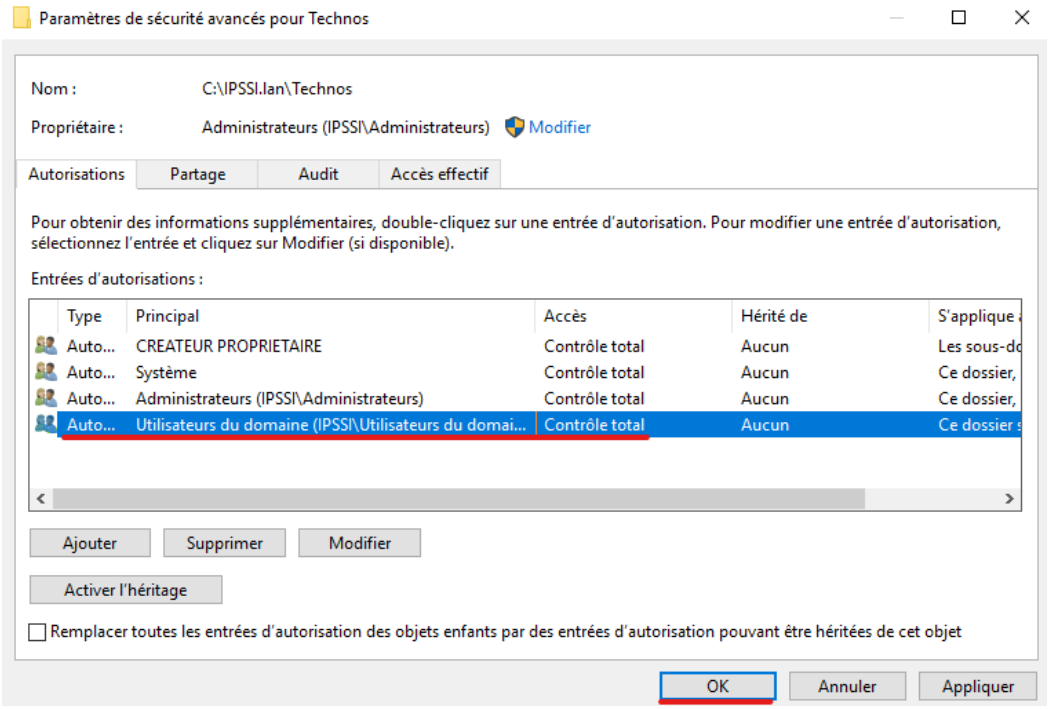
Nous mettons « utilisateurs du domaine » conformément au tableau, puis nous cliquons sur « ok ».

Etape 12



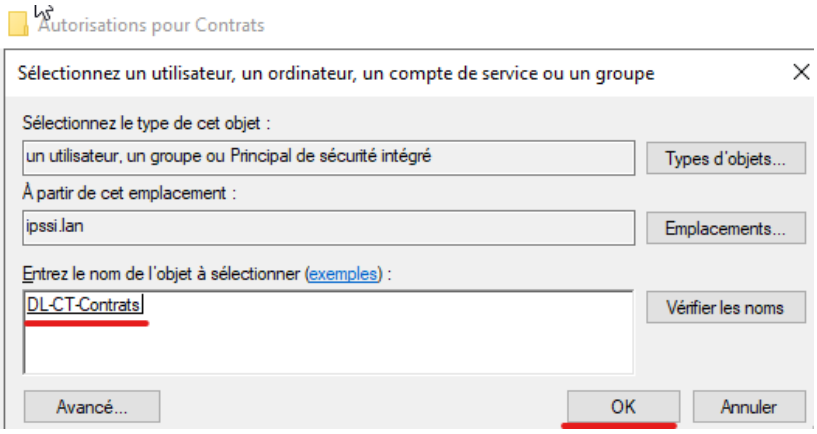
Nous appliquons cette autorisation uniquement dans ce dossier et nous cochons la case « contrôle total ». Nous cliquons sur « ok ».

Etape 13



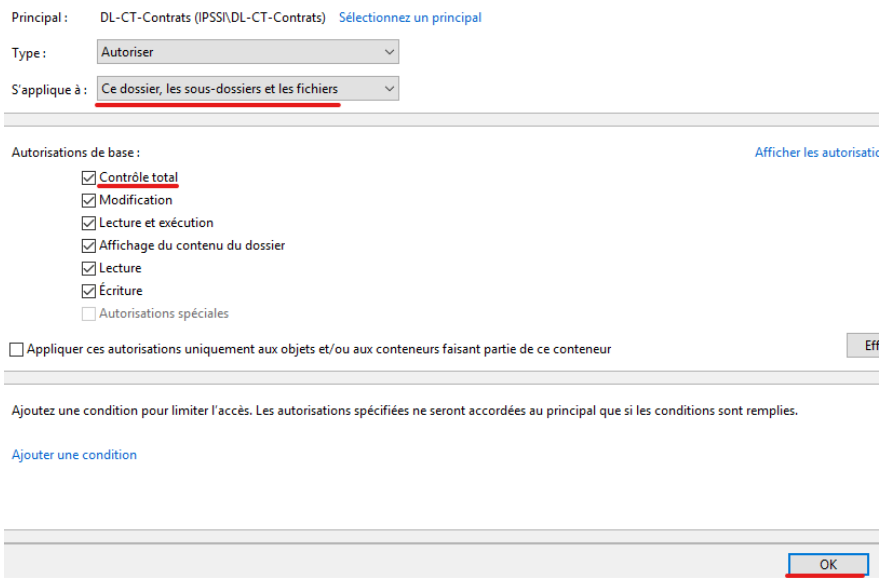
Nous voyons qu'une nouvelle est apparue, nous pouvons cliquer sur « ok ».

Etape 14



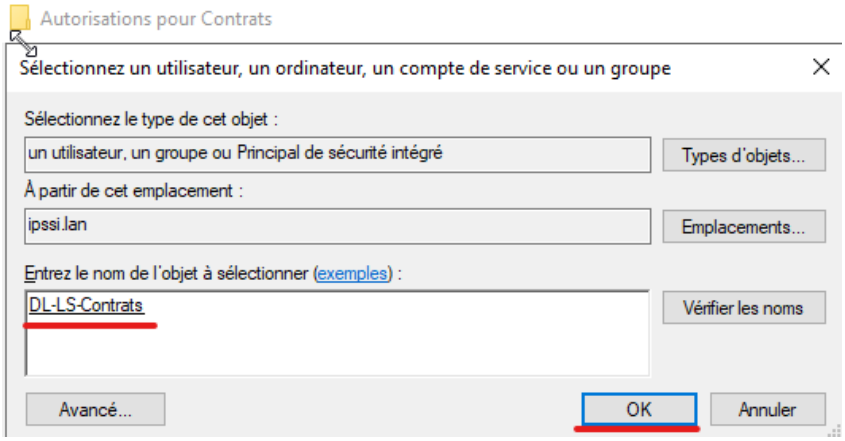
Nous allons voir comment ajouter les droits de contrôle total sur le fichier Contrats pour l'objet « DL-CT-Contrats ». Nous ajoutons de la même manière que pour le fichier Technos « DL-CT-Contrats ».

Etape 15



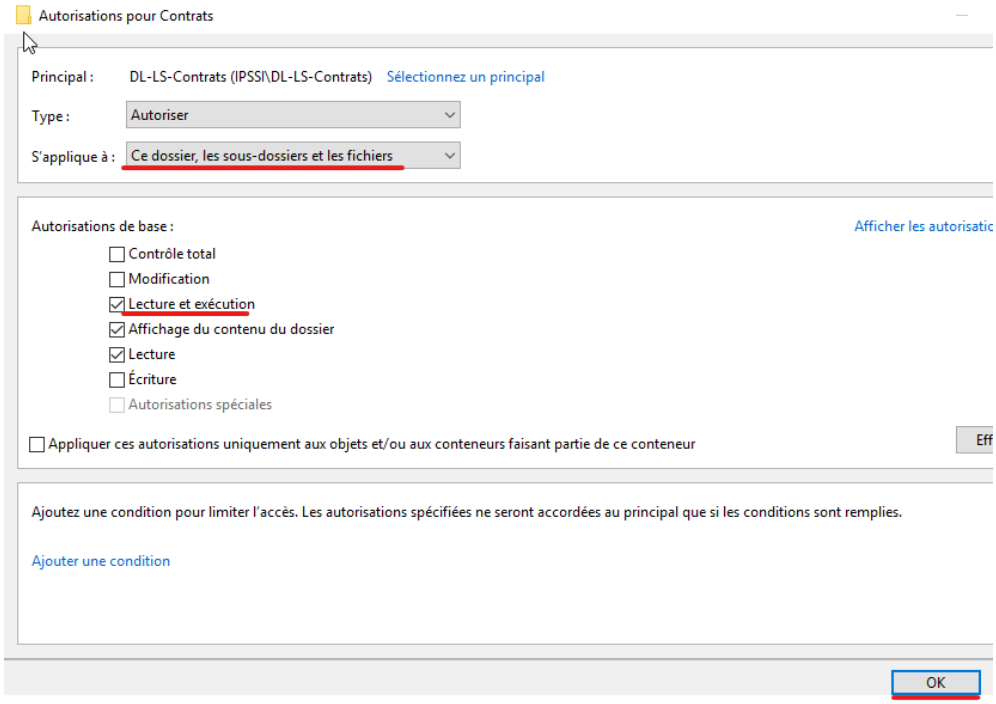
Nous sélectionnons « Contrôle total » pour ce dossier, les sous-dossiers et les fichiers.

Etape 16



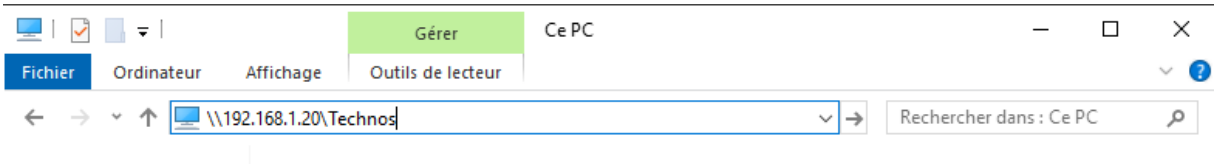
Maintenant nous allons voir pour les droits de lecture seule pour « DL-LS-Contrats ».

Etape 17



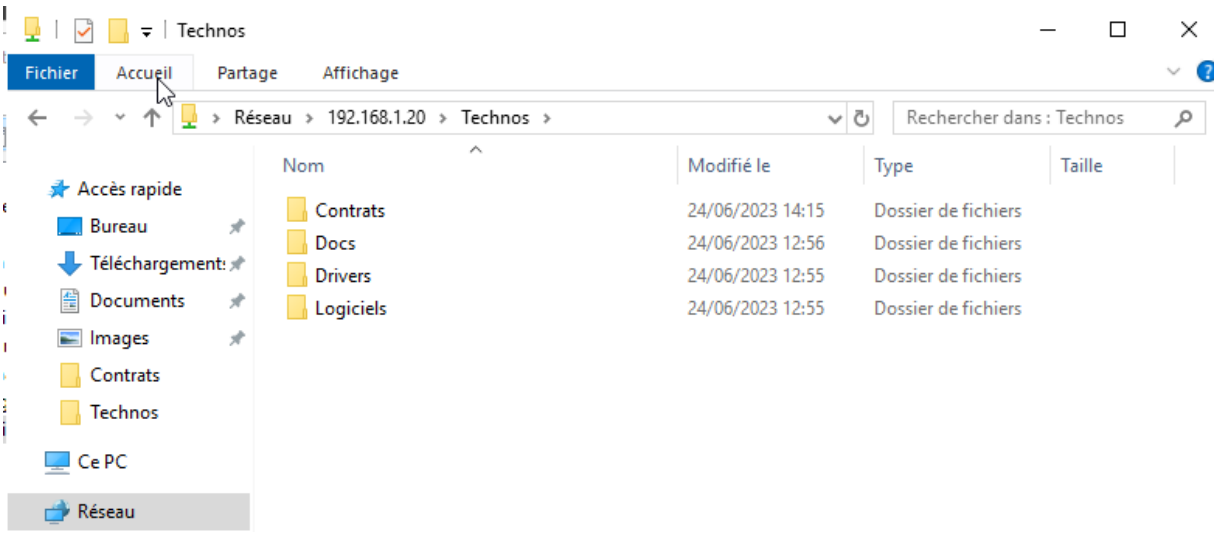
La différence consiste à sélectionner uniquement Lecture et exécution.

Etape 18



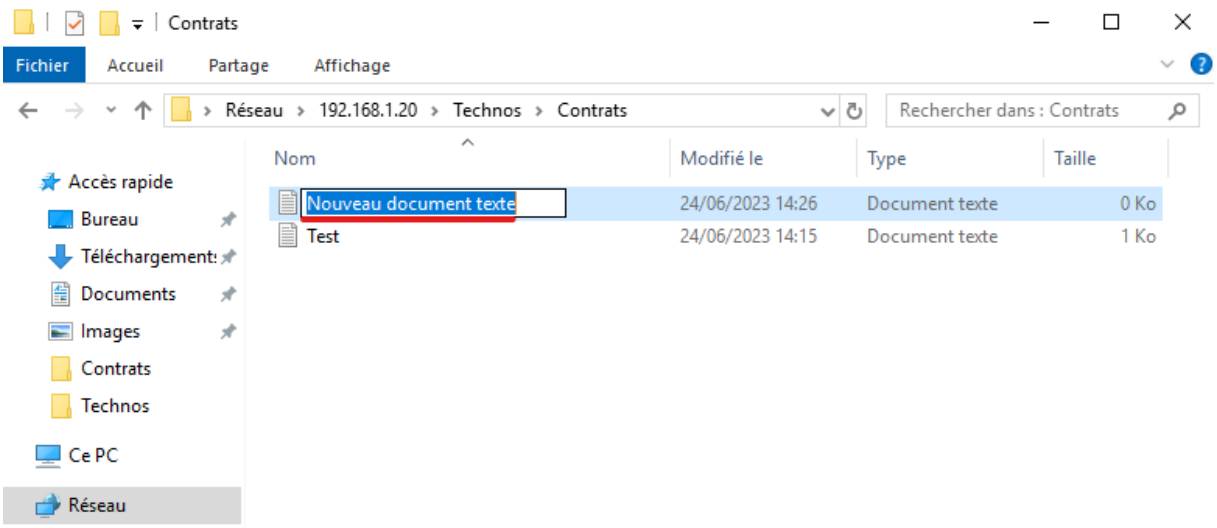
Nous nous sommes connectés sur la session de technicien1 sur W10E, puis dans l'explorateur de fichier nous avons rentré l'adresse du fichier sous le format : \\adresse_serveur\nom_du_fichier.

Etape 19



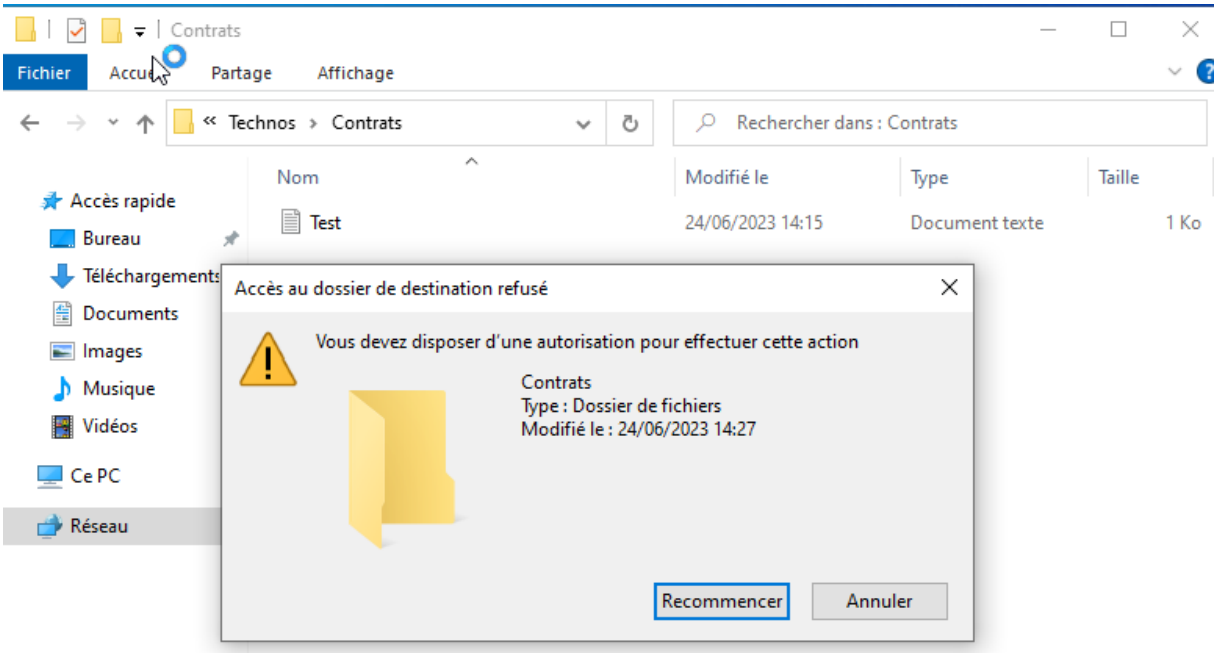
Nous voyons tous les dossiers, nous rentrons dans « Contrats ».

Etape 20



Nous pouvons ajouter un nouveau document texte. Nous avons donc bien tous les droits.

Etape 21

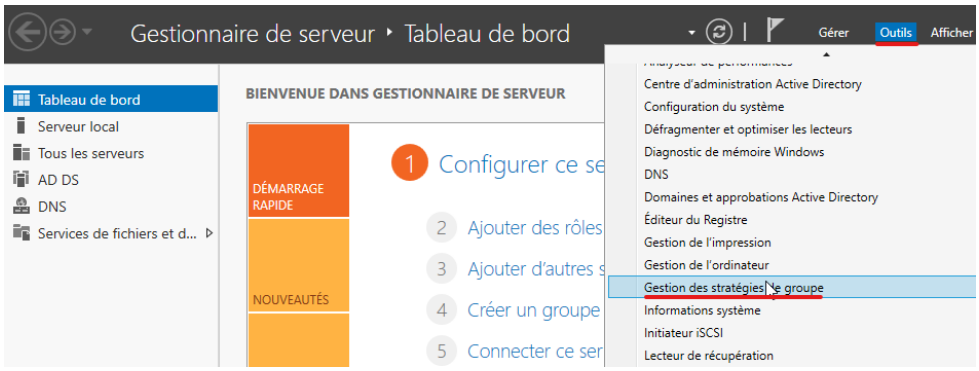


Sur la session du technicien2, nous voyons qu'il n'a les droits nécessaires pour créer un fichier.

6- Réseau partagé

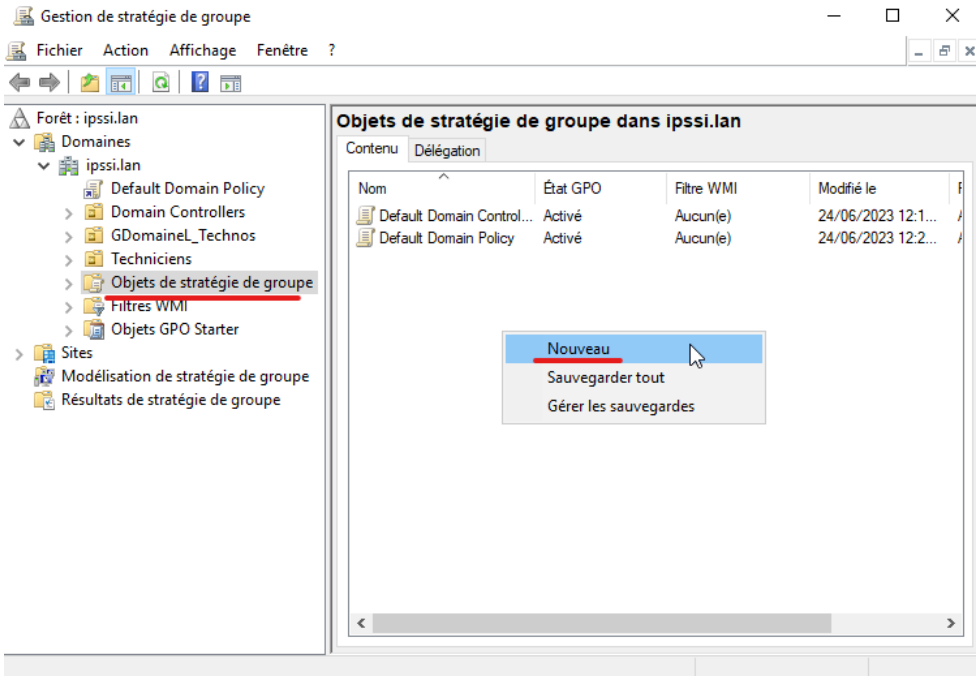
Nous allons créer une stratégie de groupe qui permettra aux techniciens d'avoir accès au lecteur contenant les fichiers technos.

Etape 1



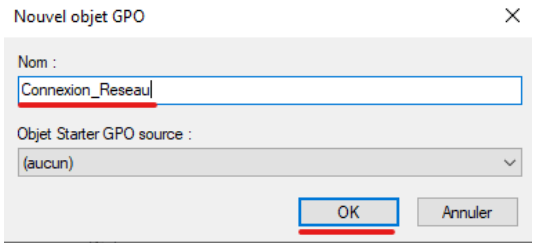
Nous nous rendons dans WS19, dans l'onglet « outils » puis « Gestion des stratégies de groupe » (GPO).

Etape 2



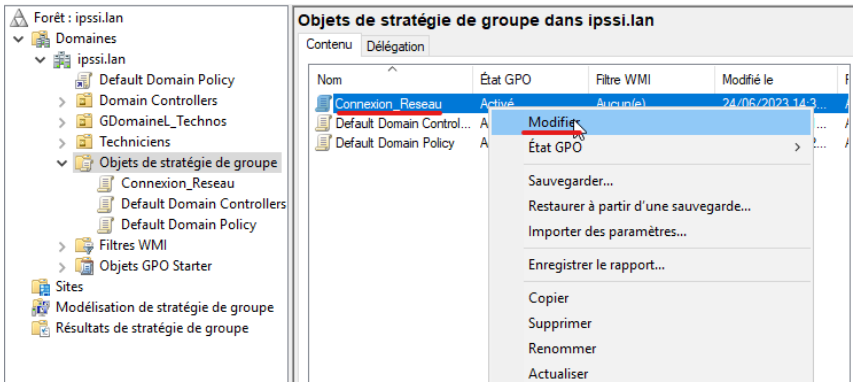
Nous déroulons l'arborescence jusqu'à « Objets de stratégies de groupe » puis nous faisons un clic-droit puis « nouveau ».

Etape 3



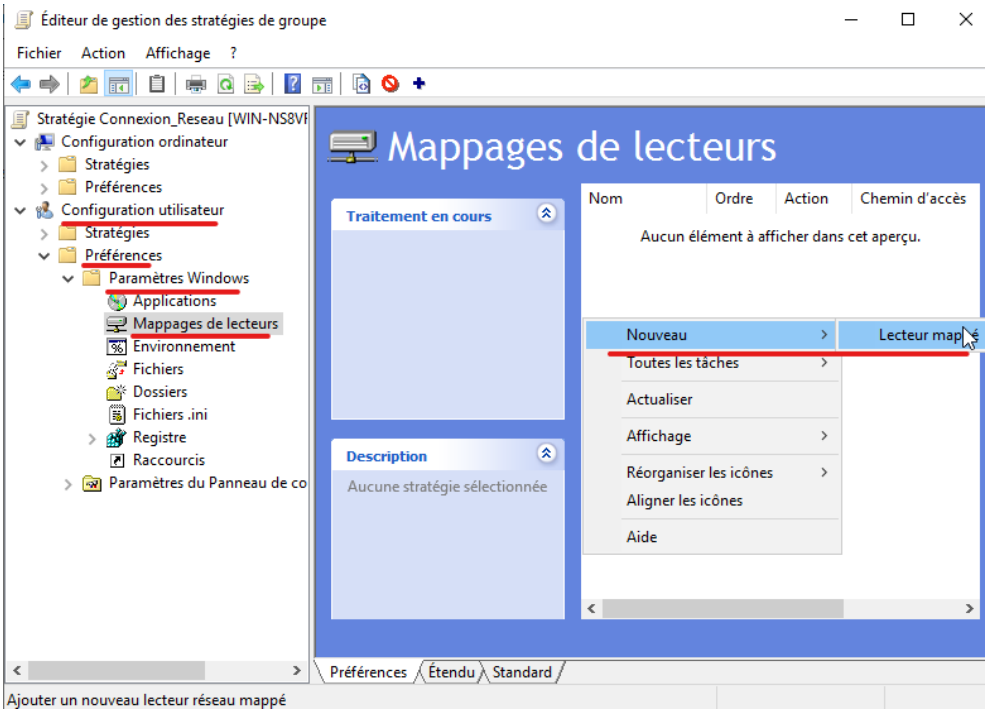
Nous nommons cette nouvelle GPO, dans notre cas « Connexion_Reseau ».

Etape 4



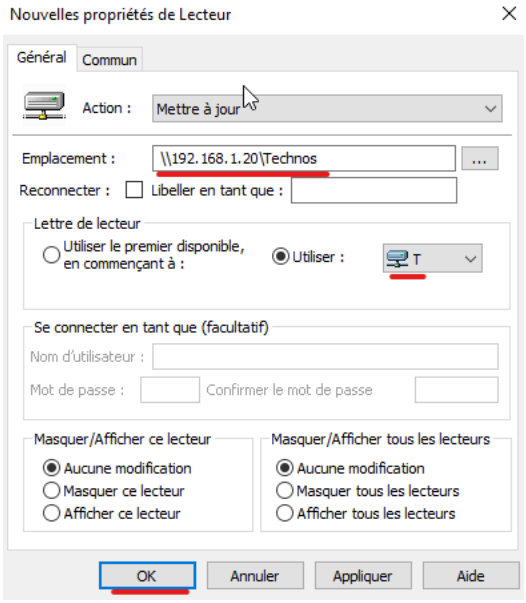
Ensuite nous faisons un clic-droit sur notre nouvelle GPO et « modifier ».

Etape 5



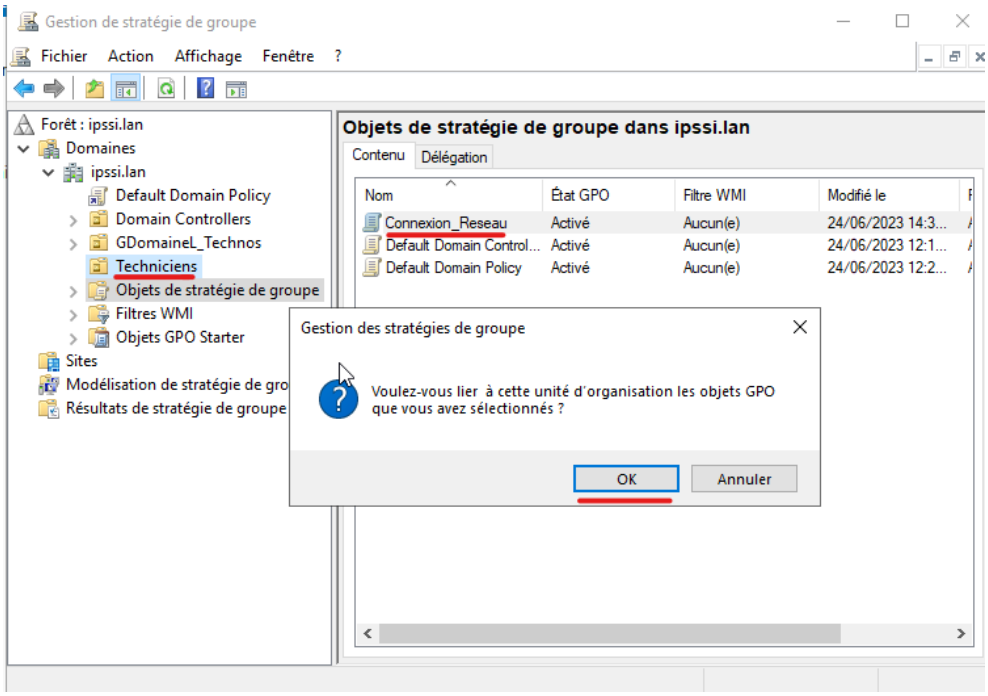
Nous déroulons l'arborescence jusqu'à « Mappages des lecteurs » puis nous créons un nouveau lecteur mappé.

Etape 6



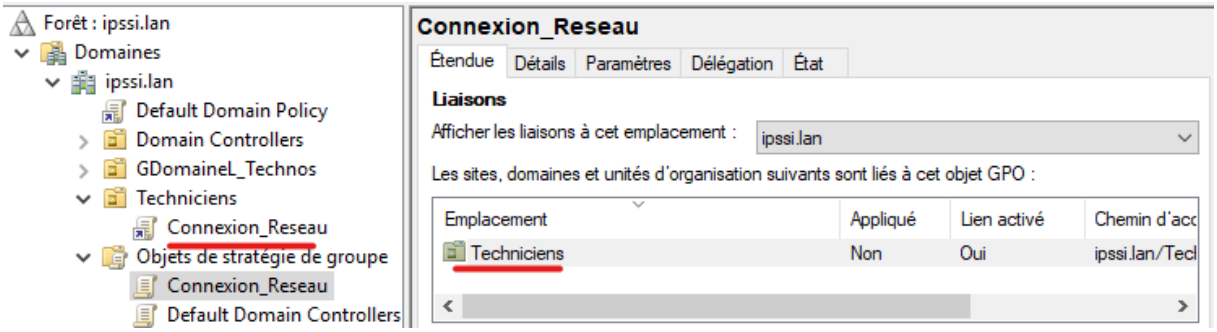
Nous indiquons le chemin vers le fichier et la lettre du lecteur.

Etape 7



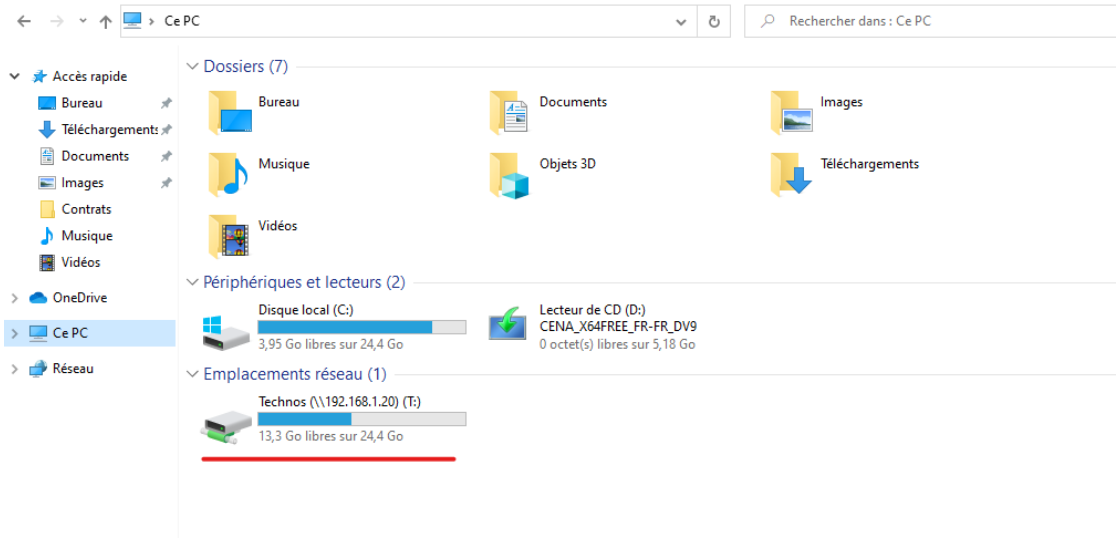
Nous lions cette GPO à l'UO « Techniciens ». Pour ce faire, nous glissons le GPO sur l'UO et nous validons cette liaison.

Etape 8



Nous voyons que la liaison est validée.

Etape 9



Sur la session de technicien1 ; nous voyons bien un nouveau lecteur contenant les fichiers créés précédemment.